National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-98
(Draft)

Guidance for Securing Radio Frequency Identification (RFID) Systems (Draft)

Recommendations of the National Institute of Standards and Technology

Tom Karygiannis
Bernard Eydt
Greg Barber
Lynn Bunn
Ted Phillips

NIST Special Publication 800-98 (Draft)

Guidance for Securing Radio Frequency Identification (RFID) Systems (Draft)

Recommendations of the National Institute of Standards and Technology

Tom Karygiannis
Bernard Eydt
Greg Barber
Lynn Bunn
Ted Phillips

C O M P U T E R S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2006

U.S. Department of Commerce

Carlos M. Gutierrez, Secretary

Technology Administration

Robert C. Cresanti, Under Secretary of Commerce for Technology

National Institute of Standards and Technology

William Jeffrey, Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. Special Publication 800-series documents report on ITL's research, guidance, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Special Publication 800-98 (Draft)
Natl. Inst. Stand. Technol. Spec. Publ. 800-98, 126 pages (September 2006)

Acknowledgments

The authors, Tom Karygiannis of the National Institute of Standards and Technology, and Bernard Eydt, Greg Barber, Lynn Bunn, and Ted Phillips of Booz Allen Hamilton, wish to thank their colleagues who reviewed drafts of this document and contributed to its technical content. The authors would like to acknowledge Tim Grance, Erika McAllister and Karen Kent of NIST, and Asterios Tsibertzopoulos, Pius Uzamere, Kenneth Waldrop, and Ted Winograd of Booz Allen Hamilton, for their keen and insightful assistance throughout the development of the document. Additional acknowledgements will be added to the final version of the publication.

SP 800-98 Note To Reviewers

NIST Special Publication 800-98, *Guidance for Securing Radio Frequency Identification (RFID) Systems*, is now available for a thirty day public comment period. SP-800-98 provides an overview of RFID technology, the associated security and privacy risks, and recommended practices that will help organizations mitigate these risks, safeguard sensitive information, and protect the privacy of individuals. Please submit comments and suggestions to sp800-98@nist.gov with "Comments on Public Draft SP 800-98" in the subject line. Reviewers are kindly requested to note the page and line number of each comment. The comment period closes at 5:00 p.m. EST (US and Canada) on October 27, 2006.

The goal of this document is to provide practical guidance on securing RFID systems using commercially available technologies. NIST is particularly interested in comments from practitioners with experience designing and implementing RFID security solutions. Comments and suggestions on the recommended management, operational, and technical Controls would be appreciated. Suggestions for additional controls that could help further mitigate the security and privacy risks and the potential impact of these controls on business processes and system performance would also be appreciated.

NIST would like to thank the reviewers in advance for sharing their expertise and valuable time to perform this public service.

Table of Contents

List of Appendices

List of Figures

List of Tables

This page has been left blank intentionally.

Executive Summary

Like any new technology, RFID presents new security and privacy risks that must be carefully mitigated through management, operational, and technical controls in order to realize the numerous benefits the technology has to offer. When practitioners adhere to sound security engineering principles, RFID technology can help a wide range of organizations and individuals realize substantial productivity gains and efficiencies. These organizations and individuals include hospitals and patients, retailers and customers, and manufacturers and suppliers throughout the supply chain. This guidance document provides an overview of RFID technology, the associated security and privacy risks, and recommended practices that will enable organizations to realize productivity improvements while safeguarding sensitive information and protecting the privacy of individuals.

Radio frequency identification (RFID) is a form of automatic identification and data capture (AIDC) technology that uses electric or magnetic fields at radio frequencies to transmit information. An RFID system can be used to identify many types of objects, such as manufactured goods, animals, and people. Each object that needs to be identified has a small object known as an RFID tag affixed to it or embedded within it. The tag has a unique identifier and may optionally hold additional information about the object. Devices known as RFID interrogators (also called readers) wirelessly communicate with the tags to identify the item connected to each tag and possibly read or update additional information stored on the tag. This communication can occur without line of sight and over greater distances than other AIDC technologies. RFID technologies support a wide range of applications—everything from asset management and tracking to access control and automated payment.

Every RFID system includes a radio frequency (RF) subsystem, which is composed of tags and interrogators. In many RFID systems, the RF subsystem is supported by an enterprise subsystem that is composed of middleware, analytic systems, and networking services. RFID systems that share information across organizational boundaries, such as supply chain applications, also have an inter-enterprise subsystem. Each RFID system has different components and customizations so that it can support a particular business process for an organization; as a result, the security risks for RFID systems and the controls available to address them are highly varied.

Implementing the recommendations presented in this publication should help organizations improve the security of their RFID systems.

Personnel responsible for designing RFID systems should understand what type of application an RFID system will support so that they can select the appropriate security controls.

Each type of application uses a different combination of components and has a different set of risks. For example, protecting financial transactions in an automated payment system requires different security controls than protecting the tracking of livestock. Factors to consider include:

- The general functional objective of the RFID technology. For example, does the system need to determine the location of an object or the presence of an object, authenticate a person, perform a financial transaction, or ensure that certain items are not separated?
- The nature of the information that the RFID system processes or generates. One application may only need to have a unique, static identifier value for each tagged object, while another application may need to store additional information about each tagged object over time. The sensitivity of the information is also an important consideration.

- The physical and technical environment at the time RFID transactions occur. This includes the distance between the interrogators and the tags, and the amount of time in which each transaction must be performed.

- The physical and technical environment before and after RFID transactions take place. For example, human and environmental threats may pose risks to tags' integrity while the tagged objects are in storage or in transit. Some applications require the use of tags with sensors that can track environmental conditions over time, such as temperature and humidity.

- The economics of the business process and RFID solution. The economic factors for RFID systems are different than those for traditional Information Technology (IT) systems. For example, many RFID tags offer few or no security features; selecting tags that incorporate basic security functionality significantly increases the cost of tags, especially if encryption features are needed. Also, the operational cost of some basic IT security controls, such as setting unique passwords and changing them regularly, may be higher for RFID systems because of the logistical challenges in managing security for thousands or millions of tags.

For RFID implementations to be successful, organizations should effectively manage their risk.

RFID technology enables an organization to significantly change its business process to increase its efficiency and effectiveness. This technology is complex and combines a number of different computing and communications technologies. Both the changes to business process and the complexity of the technology generate risk. The major high-level risks associated with RFID systems are as follows:

- *Business process risk*. Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable. For example, a warehouse that relies on RFID to automatically track items removed from its inventory may not be able to detect theft if the RFID system fails.

- *Business intelligence risk*. An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system. For example, an adversary might use an interrogator to determine whether a shipping container holds expensive electronic equipment, and then target the container for theft when it gets a positive reading.

- *Privacy risk*. The misuse of RFID technology could violate personal privacy when the RFID application calls for personally identifiable information to be on the tag or associated with the tag. For example, if a person carries products that contain RFID tags, those tags may be surreptitiously read by an adversary. This could reveal that person's personal preferences such as where they shop, or what brands they buy, or it might allow them to track that person's location at various points in time.

- *Externality risk*. RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people. For example, an adversary could gain unauthorized access to computers on an enterprise network through Internet Protocol (IP) enabled interrogators if the interrogators are not designed and configured properly. Multiple RFID interrogators operating in a confined space may cause hazards of electromagnetic radiation to fuel, ordinance or people in the vicinity.

Organizations need to assess the risks they face and choose an appropriate mix of management, operational, and technical security controls for their environments. These organizational assessments should take into account many factors, such as regulatory requirements, the magnitude of each threat, and cost and performance implications of the technology or operational practice.

When securing an RFID system, organizations should select security controls that are feasible with the RFID technologies they currently deploy or purchase new RFID technologies that support the necessary controls.

To be most effective, RFID security controls should be incorporated throughout the entire life cycle of RFID solutions—from policy development to operations. However, many RFID products support only a fraction of the possible protection mechanisms. Tags, in particular, have very limited computing capabilities. Most tags supporting asset management applications do not support authentication, access control, or encryption techniques commonly found in other business IT systems. RFID standards specify security features including passwords to protect access to certain tag commands and memory, but the level of security offered differs across these standards. Vendors also offer proprietary security features, including proprietary extensions to standards-based technologies, but they are not always compatible with other components of the system. Careful planning and procurement is necessary to ensure an organization's RFID system meets its security objectives.

This page has been left blank intentionally.

1. Introduction

1.1 Authority

The National Institute of Standards and Technology (NIST) developed this document in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets; but such standards and guidelines shall not apply to national security systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), "Securing Agency Information Systems," as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in A-130, Appendix III.

This guideline has been prepared for use by Federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority, nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official.

1.2 Purpose and Scope

This publication seeks to assist organizations in understanding the risks of RFID technology and security measures to mitigate those risks. It provides practical, real-world guidance on how to initiate, design, implement and operate RFID solutions in a manner that mitigates security and privacy risks. The document also provides background information on RFID applications, standards, and system components to assist in the understanding of RFID security risks and controls.

This document presents information that is independent of particular hardware platforms, operating systems, and applications. The emphasis is on RFID solutions that are based on industry and international standards, although the existence of proprietary approaches is noted when they offer relevant security features not found in current standards. Readers are encouraged to supplement this document with vendor publications and other materials if interested in further pursuing proprietary approaches.

Section 6 provides a brief overview of privacy laws and regulations that pertain to Federal agencies. Privacy concerns involve legal and policy issues that are addressed more thoroughly in the documents referenced in that section. Nevertheless, security and privacy concerns are not entirely separable. For instance, security mechanisms designed to protect data confidentiality also serve privacy interests. On the other hand, approaches to privacy protection that involve the temporary or permanent disabling of RFID technology may introduce a security vulnerability because of the potential for these mechanisms to be used in an unauthorized or unanticipated fashion.

This publication primarily focuses on asset management, tracking, matching, process control, and supply-chain RFID applications. RFID technology is also used in contactless smart cards that support personal identification, access control, and automated payment applications. While this document provides

information relevant to contact smart card applications, it does not address the advanced authentication and cryptography features that are incorporated into many of them.[1]

This document has been created for executives, planners, systems analysts, security professionals, and engineers who are responsible for Federal government business processes or information technology (IT) systems. Professionals with similar responsibilities outside the government should also benefit from the information this document provides. The document addresses both the needs of those considering an RFID implementation and those with an existing RFID solution. The document is also useful for researchers, students, journalists, market analysts and others who seek an overview of RFID technology and related security issues.

1.3 Document Structure

The remainder of this document is organized into seven major sections:

- Section 2 provides an introduction to RFID technology and the major components of RFID systems.
- Section 3 provides an overview of types of RFID applications. It then explains how organizations can identify application requirements to help determine which RFID technology would be most effective for a particular application.
- Section 4 discusses some of the major business risks associated with implementing RFID technology.
- Section 5 explains the various RFID security controls, including their benefits and limitations.
- Section 6 provides a brief overview of privacy regulations and controls, particularly as they pertain to Federal agencies.
- Section 7 provides recommendations that organizations using RFID systems can follow throughout the system life cycle, from initiation through operations to disposition.
- Section 8 presents two hypothetical case studies that illustrate how the concepts and recommendations introduced earlier in the document could work in practice.

Readers that are already familiar with RFID and primarily are interested in the security aspects of the technology may wish to skip Sections 2 and 3 of this document and start with Section 4.

The document also contains several appendices with supporting material. Appendix A contains more detailed information on common RFID standards. Appendices B and C contain a glossary and acronym list, respectively. Appendix D lists print resources and online tools and resources that may be useful references for gaining a better understanding of RFID technology and security.

[1] The distinction between RFID tags and contactless smart cards is becoming more difficult to define because the computing resources and security functionality of RFID tags is increasing over time. RFID tags and contacttless smartcards often use the same air interface standards and techniques for wireless communication.

2. RFID Technology

This section provides an introduction to RFID technology. It begins with a discussion of the benefits of RFID relative to other automatic identification and data capture (AIDC) technologies. It then reviews the basic components of RFID systems and provides background information needed to understand later material in the document. Readers who already have a strong understanding of RFID technology and applications can skip this section and the discussion in Section 3 about RFID applications.

2.1 Automatic Identification and Data Capture (AIDC) Technology

Identification processes that rely on AIDC technologies[2] are significantly more reliable and less expensive than those that are not automated. The most common AIDC technology is bar code technology, which uses optical scanners to read labels.[3] Most people have direct experience with bar codes because they have seen cashiers scan items at supermarkets and retail stores. Bar codes are an enormous improvement over ordinary text labels because personnel are no longer required to read numbers or letters on each label or manually enter data into an IT system; they just have to scan the label. The innovation of bar codes greatly improved the speed and accuracy of the identification process and facilitated better management of inventory and pricing when coupled with information systems.

RFID represents a significant technological advancement in AIDC because it offers advantages that are not available in other AIDC systems such as barcodes. RFID offers these advantages because it relies on radio frequencies to transmit information rather than light, which is required for optical AIDC technologies. The use of radio frequencies means that RFID communication can occur:

Like bar codes in an earlier time, RFID is the next revolution in AIDC technology. Most of the advantages of RFID are derived from the reliance on radio frequencies rather than light (as is required in optical technology) to transmit information. This characteristic means that RFID communication can occur:

- Without optical line of sight, because radio waves can penetrate many opaque materials,
- At greater speeds, because many tags can be read quickly, whereas optical technology often requires time to manually reposition objects to make their bar codes visible, and
- Over greater distances, because many radio technologies can transmit and receive signals more effectively than optical technology under most operating conditions.

The ability of RFID technology to communicate without optical line of sight and over greater distances than other AIDC technology further reduces the need for human involvement in the identification process. For example, several retail firms have pilot RFID programs to determine the contents of a shopping cart without removing each item and placing it near a scanner, as is typical at most stores today. In this case, the ability to scan a cart without removing its contents could speed up the checkout process, thereby decreasing transaction costs for the retailers. This application of RFID also has the potential to significantly decrease checkout time for consumers.

RFID products often support other features that bar codes and other AIDC technologies do not have, such as rewritable memory, security features, and environmental sensors that enable the RFID technology to record a history of events. The types of events that can be recorded include temperature changes, sudden

[2] AIDC technologies are also known as Automatic Identification Systems and Automatic Identification Technologies. The terms “automated” and “automatic” are often used interchangeably.

[3] Other AIDCs include smart cards, optical memory cards, contact memory buttons, and satellite tracking systems.

shocks, or high humidity. Today, people typically perceive the label identifying a particular object of interest as static, but RFID technology can make this label dynamic or even "smart" by enabling the label to acquire data about the object even when people are not present to handle it.

2.2 RFID System Components

RFID systems can be very complex, and implementations vary greatly across industries and sectors. For purposes of discussion in this document, an RFID system is composed of up to three subsystems:

- An *RF subsystem*, which performs identification and related transactions using wireless communication,
- An *enterprise subsystem*, which contains computers running specialized software that can store, process, and analyze data acquired from RF subsystem transactions to make the data useful to a supported business process, and
- An *inter-enterprise subsystem*, which connects enterprise subsystems when information needs to be shared across geographic or organizational boundaries.

Every RFID system contains an RF subsystem, and most RFID systems also contain an enterprise subsystem. An RFID systems supporting a *supply chain* is a common example of an RFID system with an inter-enterprise. In a supply chain application, a tagged product is tracked throughout its life cycle, from manufacture to final purchase, and sometimes even afterwards (e.g., to support service agreements or specialized user applications).

Sections 2.3 through 2.5 review each of the subsystems in more detail.

2.3 RF Subsystem

To enable wireless identification, the *RF subsystem* consists of two components:

- RFID *tags* (sometimes referred to as *transponders*), which are small electronic devices that are affixed to objects or embedded in them. Each tag has a unique identifier and may also have other features such as memory to store additional data, environmental sensors, and security mechanisms.
- RFID *interrogators* (often called *readers*), which are devices that wirelessly communicate with tags to identify the item connected to each tag and possibly associate the tagged item with related data.

Both the tag and interrogator are two-way radios. Each has an antenna and is capable of modulating and demodulating radio signals. Figure 2-1 shows a simple RF subsystem configuration.

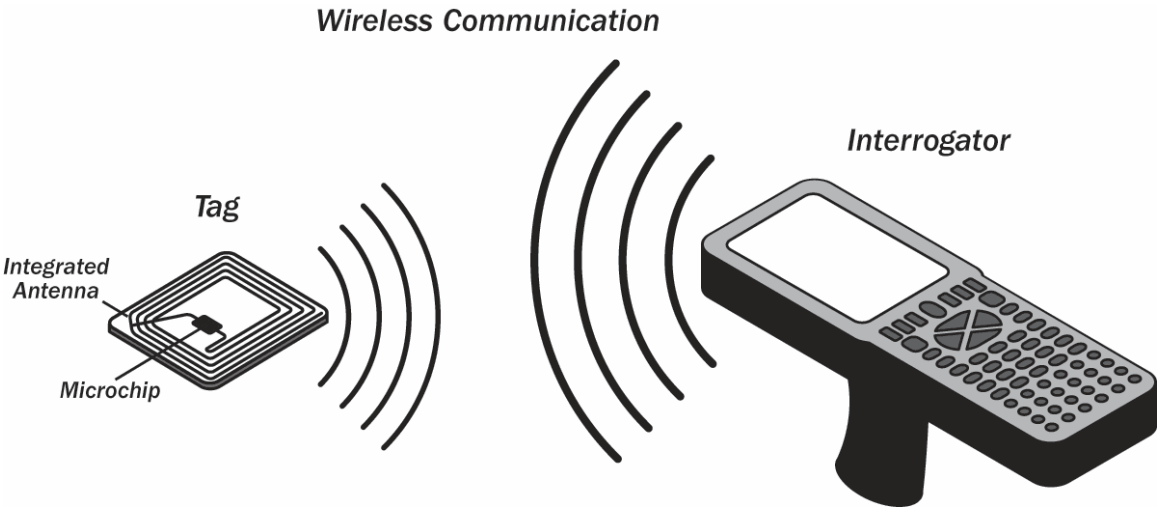

Figure 2-1. An Example of a Simple RF Subsystem

Sections 2.3.1 and 2.3.2 discuss tag and interrogator characteristics in more detail. Section 2.3.3 explains the fundamentals of tag-interrogator communication.

2.3.1 Tag Characteristics

The market for RFID tags includes over 500 different types of tags, which differ greatly in their cost, size, performance, and security mechanisms. Even when tags are designed to comply with a particular standard, they are often further customized to meet the requirements of specific applications. Understanding the major tag characteristics can help those responsible for RFID systems identify the tag characteristics required in their environments and applications. Major characteristics of tags include:

- Identifier format,
- Power source,
- Operating frequencies,
- Functionality,
- Form factor, and
- Communication protocol.

Sections 2.3.1.1 through 2.3.1.5 examine these characteristics in detail.

2.3.1.1 Identifier Format

Every tag has an identifier that is used to uniquely identify it. There are a number of data formats available for encoding identifiers on tags. System designers often want to use identifiers that have a standard structure, with certain groups of bits representing particular fields. A tag identifier format that is gaining in acceptance and use in manufacturing and retailing is the Electronic Product Code (EPC), which has four data fields:

- The *Header*, which signifies the format of the EPC identifier,

- The *Domain Manager* bits, which describe the organization that is responsible for assigning the object class and serial number bits (often the manufacturer of the item),
- The *Object Class*, which identifies a class of objects, such as a certain model of television set, and
- The *Serial Number*, which uniquely describes the instance of that class of objects (e.g., a particular television set).

Using a standard identifier format makes it easier for organizations to decode identifiers. When a machine reads a standard identifier, it can parse the identifier and decode its fields. The machine may need to request information from a remote computer to look up an identifier. When the database is distributed across several organizations and many servers, a standard identifier format with specified fields greatly facilitates the look up process. Therefore, standard identifier formats should be used whenever an RFID system will be used across multiple organizations.

If an organization does not expect its tag identifiers to be read by external parties and is concerned that the association of a tag with the organization or specific classes of objects is a business risk, then it may develop and implement its own identifier format to hide this information. Options include random or serialized identifiers that do not reveal information about the tagged item (e.g., its object class). Proprietary identifier formats can be encoded on many standards-based tags. These tags reserve memory for standard identifier formats but the memory does not have to be used for that purpose.

The data format chosen for an RFID system should be adequate for the entire life cycle of the system. Certain data formats may not have enough bits to uniquely encode all the tags that will be used in a particular application. For example, a supply chain RFID system may need longer identifiers to identify the large number of items that it will manage. The identifier data format also has security implications. For example, standard formats such as EPC allow an adversary to quickly obtain intelligence about a business activity by decoding the manager and object class fields.[4]

2.3.1.2 Power Source

Tags need power to send radio signals to an interrogator. Many tags also need power to store data, retrieve data, or perform computations. The power requirements of a tag depend on several factors, including the operating distance between the tag and the interrogator, the radio frequency being used, and the functionality of the tag. In general, the more complex the functions the tag supports, the greater its power requirements. For example, tags that support cryptography or authentication require more energy than tags that are limited to transmitting an identifier.

Tags are categorized into four types based on the power source for communication and other functionality:

- Passive,
- Active,
- Semi-active, and
- Semi-passive.

[4] The U.S. Department of Defense (DoD) has mitigated this risk by using a serialized single-field tag identifier. This serialized identifier does not reveal any information about the object with which it is associated.

A *passive tag* uses the electromagnetic energy it receives from an interrogator's transmission to reply to the interrogator. The reply signal from a passive tag, which is also known as the *backscattered signal*,[5] has only a fraction of the power of the interrogator's signal. This limited power significantly restricts the operating range of the tag. Since passive tags are low power devices, they can only support data processing of limited complexity. On the other hand, passive tags typically are cheaper, smaller, and lighter than other types of tags, which are compelling advantages for many RFID applications.

An *active tag* relies on an internal battery for power. The battery is used to communicate to the interrogator, to power on-board circuitry, and to perform other functions. Active tags can communicate over greater distance than other types of tags, but they have a finite battery life and are generally larger and more expensive. Since these tags have internal power, they can respond to lower power signals than passive tags.

A *semi-active tag* is an active tag that remains dormant until it receives a signal from the interrogator to wake up. The tag can then use its battery to communicate with the interrogator. Like active tags, semi-active tags can communicate over a longer distance than passive tags. Their main advantage relative to active tags is that they have a longer battery life. The waking process, however, sometimes causes an unacceptable time delay when tags pass interrogators very quickly or when many tags need to be read within a very short period of time.

A *semi-passive tag* is a passive tag that uses a battery to power on-board circuitry, but not to produce return signals. When the battery is used to power a sensor, they are often called *sensor tags*. They typically are smaller and cheaper than active tags, but have greater functionality than passive tags because more power is available for other purposes. Some literature uses the terms "semi-passive" and "semi-active" interchangeably.

2.3.1.3 Operating Frequencies

The radio frequencies at which a tag transmits and receives signals have implications for:

- **The operating range of the signal and the speed of tag reads and RFID data transfer.** In general, as a tag's operating frequency increases, its signals are able to carry more data.[6] As a result, higher frequency interrogators are also able to read more tags in a given period of time. In addition, RFID systems that operate at ultra high frequency (UHF) and microwave frequencies are typically designed to have a longer operating range than LF and high frequency (HF) systems.[7] For most applications, the increased speed and operating range are considered advantages. One exception is applications for which security is a significant concern, such as those that involve financial transactions or personal data. In these cases, the ability of an adversary to read the data more quickly and from a longer distance typically is considered a risk that requires mitigation.

---

[5] Passive tags that transmit ultra high frequency (UHF) or microwave signals typically rely on backscattering to communicate. Passive tags that transmit low frequency (LF) or high frequency (HF) signals typically are inductively coupled and do not communicate via backscatter.

[6] For example, EPC Class-1 Generation-2 UHF RFID technology can read tags at a speed of up to 640 kilobits per second. This data transfer rate can allow up to several hundred tags to be read per second.

[7] UHF and microwave RFID systems are typically designed to operate outside the near field of the electromagnetic signal – i.e., beyond a small number of wavelengths. This permits these systems to have a longer operating range than LF and HF systems, which generally operate in the near field. For example, EPC UHF RFID systems have a operating range of up to 15 feet, which is significantly greater than UHF wavelengths of between 0.1 and 1.0 meters (m) (approximately 4 to 39 inches). ISO 14443 HF systems have a normative range of 10 centimeters (approximately 4 inches), which is significantly less than the HF wavelengths of between 10 and 100 meters.

- **The ability of the tag's signal to penetrate materials.** As a general rule, higher frequencies are less able to penetrate substances such as metals or liquids than lower frequencies. Depending on the application, the penetration capabilities of a particular frequency can be either a benefit or a shortcoming. For example, LF communication typically is a requirement when tags are placed inside an animal (or humans, in some emerging medical applications) because RF attenuation in living tissue, which is mostly water, increases significantly as frequency increases. In applications in which security is a significant concern, an organization may want to use a frequency range than can be blocked by a particular material because this enables effective security shielding that might not otherwise be available. Table 2-1 summarizes the ability of RF signals to penetrate various substances.

- **The likelihood of radio interference.** Radio interference is another reason why transmitted signals may not be properly received. Determining the potential sources of radio interference for a particular RFID implementation requires a site survey. Nearly all RFID systems operate in non-licensed frequency bands, and they may experience radio interference from other systems that share the same frequency band. For example, wireless networking equipment, cordless telephones, and other wireless consumer devices use the microwave 2.45 and 5.8 gigahertz (GHz) bands, so they represent a potential source of interference for RFID systems that use these frequencies.

- **The international portability of tags.** The types of systems that use various portions of the electromagnetic spectrum can differ from jurisdiction to jurisdiction because not all regulators assign the same frequencies for the same purposes. If an RFID application requires transporting tags across multiple regulatory jurisdictions, then the system needs to use a frequency range permitted in all of the jurisdictions. Regulations impacting RFID often change, so organizations that use or plan to use RFID technology internationally should monitor relevant developments. Currently, there are frequencies within the LF, HF, and UHF bands that are permitted in most jurisdictions. Also, some tags are frequency-agile, so they can respond to one frequency in one jurisdiction and another in a different jurisdiction. For example, EPC Class-1 Generation-2 tags operate in the UHF band from 860 to 960 megahertz (MHz). In the United States, regulations permit operation from 902 to 928 MHz. In Europe, the typical operating range is from 865.6 to 867.6 MHz. U.S. and European interrogators can be tuned to corresponding permitted frequencies, but the tags will respond to both.

Table 2-1. Impact of Selected Materials on RF Transmissions[8]

Material	LF 30-300 kilohertz (kHz)	HF 3-30 MHz	UHF 300 MHz-1 GHz	Microwave > 1 GHz
	125 or 134 kHz (common U.S. RFID usage)	13.56 MHz[9] (Worldwide ISM band)	433.5-434.5 915 MHz[10] (common U.S. RFID usage)	2.45 or 5.8 GHz[11] (Worldwide ISM band)
Clothing	Transparent	Transparent	Transparent	Transparent
Dry Wood	Transparent	Transparent	Transparent	Absorbent
Graphite	Transparent	Transparent	Opaque	Opaque
Metals	Transparent	Transparent	Opaque	Opaque
Motor Oil	Transparent	Transparent	Transparent	Transparent
Paper Products	Transparent	Transparent	Transparent	Transparent
Plastics	Transparent	Transparent	Transparent	Transparent
Water	Transparent	Transparent	Absorbent	Absorbent
Wet Wood	Transparent	Transparent	Absorbent	Absorbent

2.3.1.4 Functionality

The primary function of a tag is to provide an identifier to an interrogator, but many types of tags support additional capabilities that are valuable for certain business processes. These include:

- **Memory.** Memory enables data to be stored on tags and retrieved at a later time. Memory is either write once, read many (WORM) memory or re-writeable memory, which can be modified after initialization. Memory enables more flexibility in the design of RFID systems because RFID data transactions can occur without concurrent access to data stored in an enterprise subsystem. However, adding memory to a tag increases its cost and power requirements. Section 3 discusses RFID application requirements and provides additional information about the circumstances under which the use of re-writable memory would be a desirable approach.

- **Environmental sensors.** The integration of environmental sensors with tags is an example of the benefit of local memory. The sensors can record temperature, humidity, vibration, or other phenomena to the tag's memory, which can later be retrieved by an interrogator. The integration of sensors significantly increases the cost and complexity of the tags. Moreover, while many tag operations can be powered using the electromagnetic energy from an interrogator, this approach is not workable for sensors, which must rely on battery power. Tags typically are only integrated with sensors for high-value, environmentally sensitive, or perishable objects worthy of the additional expense.

[8] Lahiri, Sandip. RFID Sourcebook. IBM Press. 2005.

[9] This is the designated center frequency for the frequency band of 13.553-13.567 MHz, which is an Industrial, Scientific, and Medical (ISM) band that is available worldwide.

[10] The designation 915 MHz represents the frequency band of 902 – 928 MHz, which is an ISM band in Region 2. Contrarily, 433.5 – 434.5 MHz is not an ISM band but RFID systems in the United States can use this band subject to restrictions in the Federal Communications Commission (FCC) Part 15 rules.

[11] The designation of 2.4 GHz represents the center frequency of the 2.400-2.500 GHz frequency band, which is an ISM band. Similarly, 5.8 GHz represents the center frequency of the 5.725 - 5.875 GHz frequency band, which is also an ISM band.

- **Security functionality, such as password protection and cryptography.** Tags with on-board memory are often coupled with security mechanisms to protect the data stored in that memory. For example, some tags support a *lock* command that, depending on its implementation, can prevent further modification of data in the tag's memory or can prevent access to data in the tag's memory. In some cases, the *lock* command is permanent and in other cases, an interrogator can "unlock" the memory. EPCglobal standards, International Organization for Standardization (ISO) standards, and many proprietary tag designs support this feature. Some RFID systems support advanced cryptographic algorithms that enable authentication mechanisms and data confidentiality features, although these functions are most commonly found on RFID-based contactless smart cards and not tags used for item management. Some tags offer tamper protection as a physical security feature.

- **Privacy protection mechanisms.** EPC tags support a feature called the *kill* command that permanently disables the ability of the tag to respond to subsequent commands. Unlike the *lock* command, the *kill* command is irreversible. The *kill* command also prevents access to a tag's identifier, in addition to any memory that may be on the tag. While the *lock* command provides security, the primary objective of the *kill* command is personal privacy. RFID tags could be used to track individuals that carry tagged items or wear tagged articles of clothing when the tags are no longer required for their intended use, such as to expedite checkout or inventory. The ability to disable a tag with the *kill* command provides a mechanism to prevent such tracking.

2.3.1.5 Form Factor

The *form factor* of a tag refers to its shape, size, packaging, and handling features. To a large extent, a tag's form factor is determined by the characteristics previously discussed, such as power source and functionality. Some important aspects regarding a tag's form factor include the size of the tag, the weight of the tag, and the method by which the tag is affixed to and removed from its associated object. Tags typically vary in size from smaller than a postage stamp to about the size of a common document stapler. Active tags typically are significantly larger and heavier than passive tags because they have an onboard power supply. Tags that integrate environmental sensors are also larger and heavier than those without this functionality. While increasing the computing functionality of a tag increases its cost and power requirements, it may not have an impact on its form factor because the microchip on a passive tag is one of the tag's smallest components. On most tags, the largest component on the tag is its antenna.

Tags can be attached to items using an adhesive or can be embedded within the item. The primary concern when a tag is attached to an item is how easily it might be detached, whether accidentally or maliciously Tags attached to items also are more vulnerable to harsh environmental conditions such as dust, debris, humidity, precipitation, and extreme temperatures. However, the vulnerability is intentional in some cases. For example, RFID tags known as *frangible tags* allow users to deactivate tags by tearing the tag's antenna from its circuitry. Figure 2-2 shows a tag printer producing tags that might have such a characteristic. Tags that are embedded in objects (e.g., smart cards, animal tissue, plastic housing) are less vulnerable to tampering and environmental conditions.

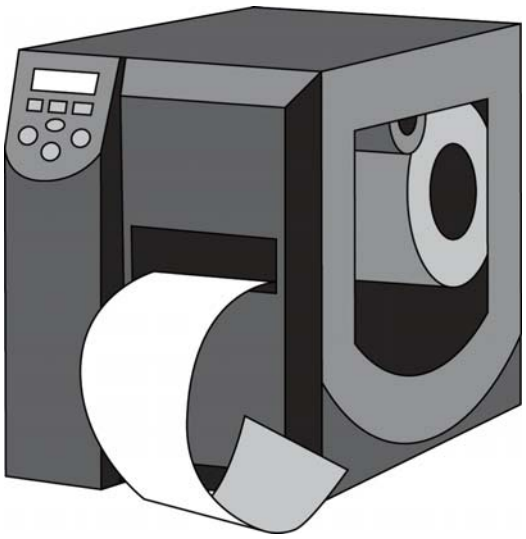

Figure 2-2. RFID Tag Printer

2.3.2 Interrogator Characteristics

The tag and the interrogator must comply with the same standard in order to communicate. If a tag is based on a proprietary design, an interrogator must support the same communication protocol to communicate with that tag. In many cases, if proprietary tags are used, only proprietary RFID readers from the same vendor can be used. Interrogator characteristics that are independent of tag characteristics include:

- Interrogator power output and duty cycle,
- Enterprise subsystem interface,
- Mobility, and
- Antenna design and placement.

These interrogator characteristics are discussed in Sections 2.3.2.1 through 2.3.2.4.

2.3.2.1 Power Output and Duty Cycle

In most cases, standards and regulations will determine the permitted power output and duty cycle of the interrogators. An interrogator's *duty cycle* is the percentage of time that the device is emitting energy over a specified period. For example, an interrogator that communicates for 30 seconds every minute has a 50% duty cycle. Interrogators that communicate with passive tags need greater power output than those that communicate with active tags because the signal must be strong enough to reach the tag and enable the backscatter to return to the interrogator. In general, interrogators with greater power output and duty cycles can read tags more accurately, more quickly, and from longer distances, but the greater power output also increase the risk of eavesdropping.

2.3.2.2 Enterprise Subsystem Interface

All interrogators have an RF subsystem interface to communicate with tags. Most also have a second interface to communicate with the enterprise subsystem. The enterprise subsystem interface supports transfer of RFID data from the interrogator to enterprise subsystem's computers for processing and

analysis. In most cases, the enterprise subsystem interface is used for remote management of the interrogators. The interface may be a wired (e.g., Ethernet) or wireless (e.g., Wi-Fi or satellite) link. Many systems use Simple Network Management Protocol (SNMP) to monitor the interrogators and alert administrators of conditions that warrant attention.

2.3.2.3 Mobility

An interrogator's interface with an enterprise subsystem may be wired or wireless. Most wired interrogators are in fixed locations and support applications in which the tags approach the interrogator. Some wired interrogators offer limited mobility using cables. Figure 2-3 shows an interrogator portal that reads tags on a pallet of boxes moving through the portal. Figure 2-4 shows interrogator antennas mounted above each toll lane in a series of toll booths. As vehicles pass through one of the toll lanes, the interrogator reads a tag transponder that is attached to that vehicle's windshield.

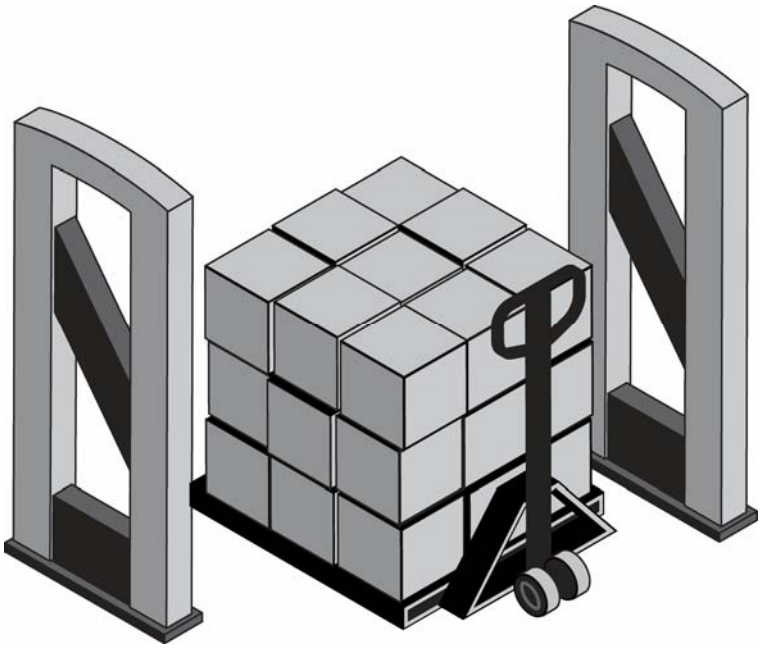

Figure 2-3. Fixed Interrogator in Item Management Application

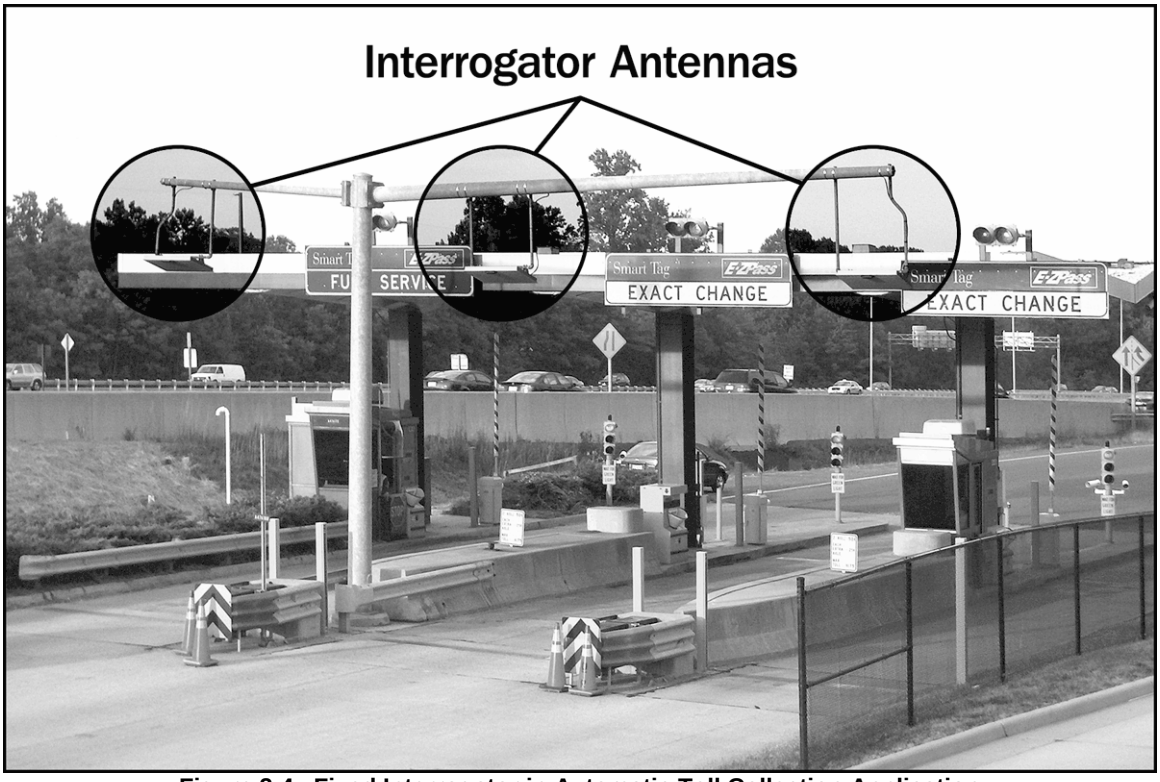

Figure 2-4. Fixed Interrogator in Automatic Toll Collection Application

In contrast, wireless interrogators support applications in which personnel must move around to read tags.[12] Figure 2-5 shows an example of a mobile handheld interrogator. A mobile interrogator usually uses different communications protocols on its RF and enterprise subsystem interfaces, even though both interfaces are wireless. Institute of Electrical and Electronics Engineers (IEEE) 802.11, also known as Wi-Fi, is a common protocol for the enterprise subsystem interface. RF interfaces are defined in RFID standards documents, such as ISO 18000.

Figure 2-5. Mobile Handheld Interrogator

[12] Wireless protocols are also used on the enterprise subsystem interface when an organization determines it is cost-prohibitive or inconvenient to extend the wired infrastructure to the interrogator.

2.3.2.4 Antenna Design and Placement

Interrogators use a wide variety of antenna types. Each type has different coverage patterns. To reduce the likelihood of eavesdropping and minimize interference with other radios, the coverage should only encompass a range sufficient to communicate with the intended tags. Antennas may be integrated into the device or may be detachable. Interrogators that support detachable antennas are better suited for applications that require specific coverage areas because an antenna can be selected or customized to meet those requirements.

Antennas can be mounted for a particular application. Figures 2-3 and 2-4 in Section 2.3.2.3 show examples of item tracking and automatic toll payment applications. Antennas can also be mounted on forklifts to identify items when they are moved from one location to another. In industrial applications, antennas are often placed in tunnels around a production line's conveyor belt.

2.3.3 Tag-Interrogator Communication

Tag-interrogator communication characteristics that affect performance and security include:

- How tag-interrogator communication is initiated,
- How an interrogator directs messages to particular tags, and
- How far away a tag or interrogator's signal can be reliably detected or interpreted.

These are discussed in detail in Sections 2.3.3.1 through 2.3.3.3.

2.3.3.1 Communication Initiation

Tags and interrogators can initiate RF transactions in two general ways:

- **Interrogator Talks First (ITF).** In an ITF transaction, the interrogator broadcasts a signal that is received by tags in the interrogator's vicinity. Those tags may then be commanded to respond to the interrogator and to continue transactions with the interrogator.
- **Tag Talks First (TTF).** In a TTF transaction, a tag communicates its presence to an interrogator when the tag is within the interrogator's RF field. If the tag is passive, then it transmits as soon as it gets power from the interrogator's signal to do so. If the tag is active, then it transmits periodically as long as its power supply lasts. This type of transaction might be used when it is necessary to identify objects that pass by an interrogator, such as objects on a conveyer belt.

Interrogators and tags in an RFID system typically operate using only ITF or only TTF transactions, not both types. TTF operation may be easier for an adversary to detect or intercept, because tags send beaconing signals even when they are not in the presence of an interrogator.

2.3.3.2 Singulation

Singulation is the process by which an interrogator identifies a particular tag. This capability is critical whenever multiple tags are in close proximity. For instance, when an interrogator issues a command to modify a tag's memory, neighboring tags should not accidentally execute the same command. Similarly, when an interrogator sends a query to a tag, the interrogator should not receive a response from multiple tags.

In the EPCglobal Class-1 Generation-2 standard, the singulation protocol requires the interrogator to transmit commands to every tag within its operating range. The interrogator asks for tags with specific memory contents to respond. When the tags respond, each provides its unique identifier and a random number that the interrogator uses to address the tag in subsequent communication. The random number has significantly fewer bits than the tag's identifier, which simplifies the processing of later transactions. A possibility exists that two tags will respond with the same random number, but the probability of this occurrence is kept low by design even in the presence of a large number of tags.

One way to thwart communication between an interrogator and a tag is to interfere with an interrogator's attempts to singulate tags. For example, when an interrogator is performing singulation, a *blocker tag* responds as if all tags with all possible identifiers were present. [13] As a result, the interrogator cannot successfully singulate any one tag. Blocker tags that travel with tagged objects may prevent illicit reading of the tags[14]. The blocker tags then would be separated from the items whenever those items need to be presented to a legitimate interrogator. However, an adversary could also use blocker tags to prevent legitimate transactions. Blocker tag technology is still under development and is not yet proven technology. Research is also being conducted on methods to thwart blocker tags.

Some RFID technologies do not support singulation. For example, ISO 11785/11784 animal tracking tags have no collision detection or avoidance mechanism because multiple tags are not usually read in close proximity for this type of application.

2.3.3.3 Signal Propagation Distance

The communications link between a tag and an interrogator is bi-directional. The interrogator transmits a signal to a tag over the *forward channel*. The tag responds on the *back channel*, which is also called the *reverse* channel or *backscatter* channel. When RFID systems use passive tags, signals on the forward channel typically are much more powerful than those on the back channel. Therefore, signals on the forward channel can be detected or properly received over longer distances. This difference has important implications for RFID communications security, including both the vulnerability of RF subsystem traffic and the mechanisms used to protect it. Some relevant operational ranges related to various communications objectives are:[15]

- **Nominal operating range**, which is the distance, often specified by standard, over which authorized transactions are expected to occur,
- **Back channel eavesdropping range**, which is the distance over which a rogue receiver can reliably interpret a tag's response to a legitimate interrogator,
- **Rogue skimming (or scanning) range**, which is the distance over which a rogue interrogator operating above regulated power limits can reliably communicate with a tag,
- **Rogue command range**, which is the distance over which a rogue interrogator can execute a tag command that does not require the interrogator to successfully receive information from the tag[16],

[13] "The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy" in V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, pp. 103-111. ACM Press. 2003.

[14] There are designs for thwarting blocker tags.

[15] Juels, A, "RFID Security and Privacy: A Research Survey," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 2, pp. 381-394, February 2006

[16] EPC Class-1 Generation-2 tags use a technique called *cover-coding* that requires that an interrogator successfully receive a message before it can issue *kill*, *lock*, and *write* commands. This technique, which is discussed in more detail in Section 5.3.2.4 and in Appendix A, in effect makes the rogue command range equivalent to the back channel eavesdropping range, thereby significantly reducing the threat of rogue commands.

- **Forward channel eavesdropping range**, which is the distance over which a rogue receiver can reliably listen to the transmissions of an authorized interrogator, and
- **Forward channel traffic analysis range**, which is the distance over which a rogue receiver can detect the presence of an interrogator's signal without having to reliably interpret its content.

Eavesdropping ranges can be significantly greater than the nominal operating ranges listed in product literature. For example, security researchers have demonstrated that the rogue scanning range of an ISO 14443 contactless smart card is at least 50 centimeters (cm), which is five times the standard's nominal operating range.[17] For some RFID technologies, forward channel eavesdropping is possible for distances on the order of kilometers.[18]

If the potential adversary does not need a reply from a passive tag to achieve its objective, then the adversary can be much farther away. For instance, for many tags, an interrogator does not need to receive a message from the tag before writing to the tag's memory. This attack is not possible for certain commands in EPC Class-1 Generation-2 tags, because mandatory cover-coding requires the interrogator to receive a key from the tag before issuing a command.[19] *Cover-coding* is a technique used to obscure the content of messages from interrogators to tags and is described in more detail in Section 5.3.2.4.

Similarly, an adversary can be further away if that adversary obtains information from the mere detection of the signal, even if the signal is too weak to reliably decode. The presence of a signal indicates that RFID activity is occurring, which an adversary could use to infer that a shipment has arrived. An adversary may also be able to determine the number of transactions taking place even if it cannot identify the nature of those transactions, but this nonetheless could be used infer the level of business activity. This type of intelligence gathering is called *traffic analysis*, and it can be performed over much greater distances than eavesdropping.

2.4 Enterprise Subsystem

The *enterprise subsystem* connects interrogators to computers running software that can store, process, and analyze data acquired from RF subsystem transactions to make the data useful to a supported business process. For example, an RFID system in a retail clothing store has an RF subsystem that can read the identifier associated with each tagged garment. The enterprise subsystem matches the identifier to the garment's record in a database to determine its price and the number of other items of a similar type that remain in inventory. Some simple RFID systems consist of an RF subsystem only (e.g., RFID-based key systems in which an interrogator can make an access control decision without access to other computers). However, most RFID systems have both an RF subsystem and an enterprise subsystem.

The enterprise subsystem consists of three major components, which are shown in Figure 2-6, and described in Sections 2.4.1 through 2.4.3:

- Middleware,
- Analytic systems, and

[17] Ilan Kirschenbaum and Avishai Wool, "How to Build a Low-Cost, Extended-Range RFID Skimmer", February 2, 2006, http://eprint.iacr.org/2006/054.pdf.

[18] Eavesdropping at this distance would require advanced monitoring equipment and ideal environmental conditions, including optical line of sight transmission, low humidity, and no radio interference.

[19] The affected commands are *kill*, which disables all subsequent tag commands; *write*, which is used to write information to a tag's memory; and *access*, which is necessary to lock memory. The technique, in effect, makes the rogue command range equivalent to the back channel eavesdropping range, thereby significantly reducing the threat of rogue commands.

- Network infrastructure.

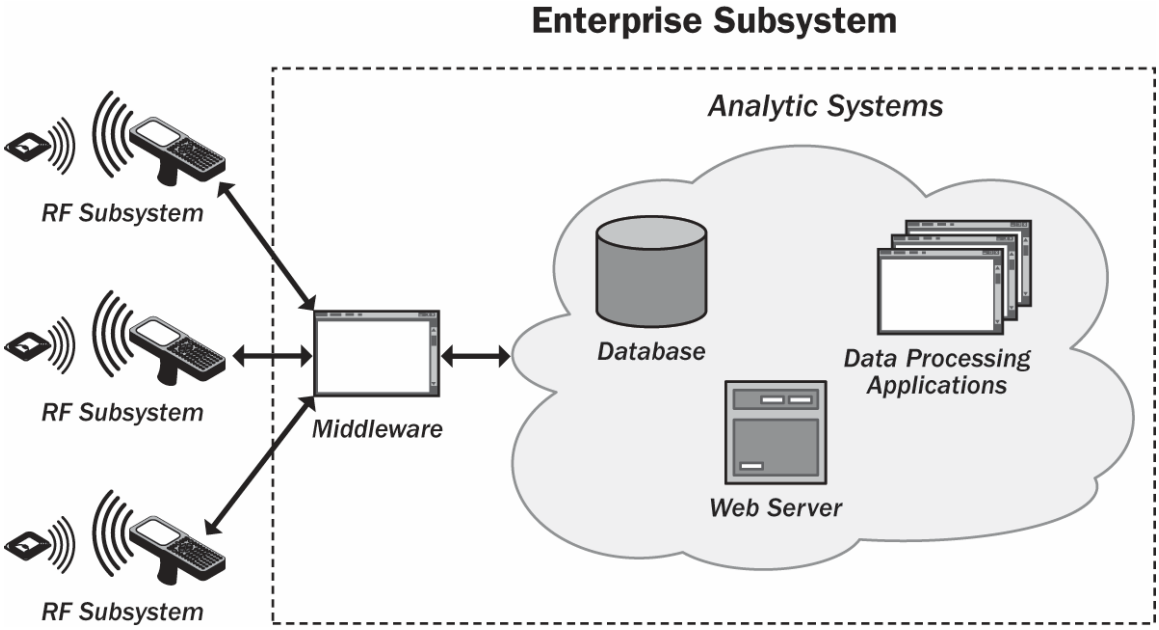

Figure 2-6. RFID System Architecture

2.4.1 Middleware

RFID *middleware* is responsible for preparing data collected from interrogators in the RF subsystem for the analytic systems that directly support business processes. Middleware hides the complexity and implementation details of the RF subsystem from the analytic systems. This allows the developers and users of the analytic systems to focus on the business implications of RFID data rather than the intricacies of wireless communication. For example, middleware filters duplicate, incomplete, and erroneous information it receives from interrogators. Middleware filtering is especially useful for applications in which large numbers of tags are in close proximity and for challenging RF environments, such as those containing reflective materials. The middleware can immediately transfer the filtered data to the analytic systems or aggregate and store it for later retrieval.

System administrators also use middleware to monitor and manage interrogators. For example, system administrators use middleware to adjust the power output and duty cycle to reduce the number of transaction errors. Many middleware products also support event-based triggers that perform actions automatically under certain conditions. Middleware transaction logs help with the identification of anomalous behavior, which could help an organization detect unauthorized use of the RFID system. Many middleware products also provide additional features, such as printing RFID labels that provide benefits beyond data and device management.

2.4.2 Analytic Systems

Analytic systems are composed of databases, data processing applications, and Web servers that process the data outputs of middleware based on business requirements and user instructions. They contain customized business logic for each business process they support. For example, the analytic systems of

an RFID system supporting logistics may include customized rules for automated inventory management, procurement, shipping, receiving, and billing.

Analytic systems are often enterprise applications that draw inputs from multiple sources, many of which may not involve the RF subsystem. For example, some RFID systems are designed to co-exist with or complement existing AIDC systems (e.g., bar code technology). Analytic systems also correlate RFID data with non-RFID business records imported from other databases, such as records from business partners, customers, logistics service providers, and suppliers. Therefore, analytic systems are often based on commercial database software or legacy applications[20] that support processing of data other than RFID data.

Analytic systems that are a part of the EPCglobal network and process data based on tags that comply with EPC standards are called *EPC information services (EPCIS)*.

2.4.3 Network Infrastructure

Network infrastructure enables communication between the RF and enterprise subsystems, as well as among components of the enterprise subsystem. Some important characteristics of network infrastructure include:

- The physical and logical topology of the network, and
- Data communications protocols.

2.4.3.1 Physical and Logical Topology

The *topology* of a network describes how network computing elements are physically and logically connected to each other. *Physical topology* describes the network's cable plant or air interfaces. *Logical topology* describes how the communications links between devices are arranged. Network communications devices often are configured so that the logical topology is different than the physical topology. For example, communications equipment can be configured to create *virtual private networks (VPN)* that logically combine and segment physical networks to achieve performance and security objectives.

The physical topology of a network infrastructure supporting an RFID system depends on the physical location of the components in its enterprise subsystem. For example, the RF to enterprise subsystem connections are physically located near interrogators.

The physical location of middleware servers depends on the level of traffic generated by the interrogators. If RFID transactions are relatively infrequent (e.g., an access control system with relatively small numbers of users), then the location of middleware is not critical. In this context, the middleware can be placed in a central location to serve multiple interrogators. If the business process requires large numbers of tags to be read quickly (e.g., multiple checkout stations in a busy store), then middleware is located near the interrogators to avoid latency problems and data throughput restrictions associated with many wide area networks. In some cases, middleware capabilities are incorporated into the communication switches to which the interrogators connect, so RFID-related traffic does not need to traverse even a single device before it is filtered and processed. This configuration is often termed an *edge processing network* because the switches are considered at the network's edges.

[20] In this context, legacy applications are computer applications that significantly predate the RFID system and are not designed to process data in formats that middleware supports. In this situation, data has to be converted into a format that the legacy application can interpret.

The physical location of analytic systems usually depends on how an organization manages its enterprise applications. If the analytic systems are dedicated to the RFID application, then organizations often place these systems near interrogators and middleware. On the other hand, some organizations locate their analytic systems in remote data centers to take advantage of the centers' physical security, on-site technical personnel, and business continuity infrastructure (e.g., electric generators, enterprise data backup, high-availability communications equipment). If the analytic systems integrate both RFID and non-RFID information systems, then it is unlikely that the location of the RF subsystem will significantly influence the location of the analytic systems.

When the enterprise subsystem components are distributed across an organization's network, the resulting physical topology can be complex, but depending on the network's configuration, the logical topology might be relatively simple. Many organizations create *virtual local area networks* (VLAN) for the distributed enterprise subsystem devices that make them appear to each other as if they were on the same network segment. VLANs reduce latency that causes performance problems on networks with large numbers of time-sensitive transactions. They also isolate traffic from other systems, which improves security.

2.4.3.2 Data Communications Protocols

Data communications protocols are a critical component of a network's performance, reliability, and security. A complete discussion of data communications protocols is beyond the scope of this guide, but readers should be able to distinguish between *link-layer* and *network-layer* protocols to understand how RFID enterprise subsystem network infrastructures work and are secured. *Link-layer* protocols specify how devices communicate with each other over a common medium, or link. *Network-layer* protocols (sometimes called *internetwork* protocols) describe how data traffic is routed across multiple network links, possibly over many types of media.

The most common link-layer protocol connecting RFID enterprise subsystem components is Ethernet (IEEE 802.3), which is the same link-layer protocol used to connect most office computers to local wired networks. Ethernet has no built-in security functionality, which means other complementary data communications protocols must provide any required protection.

In most RFID implementations, data communication within the enterprise subsystem is wired communication. The exception is mobile interrogators, which connect to the enterprise subsystem using a wireless link-layer protocol, such as Wi-Fi (IEEE 802.11). Wi-Fi's characteristics are significantly different than the link-layer protocols supporting communication between tags and interrogators. In particular, Wi-Fi equipment supporting Wi-Fi Protected Access (WPA) includes numerous security features, such as strong authentication and encryption.[21]

The most common network-layer protocol for enterprise subsystem communication is the IP. Since most modern computers are IP-enabled, enterprise subsystem components, such as middleware and analytic systems, can easily communicate across the enterprise and over external networks, including the Internet. The ability to communicate with a diverse range of computers and their application services also represents a security risk. IP-enabled enterprise subsystem components are subject to the same protocol attacks as any other IP-enabled computer.

[21] See NIST SP 800-97, *Guide to IEEE 802.11i: Establishing Robust Security Networks*, for additional information on IEEE 802.11 security, such as differences between WPA and WPA Version 2.

2.5 Inter-Enterprise Subsystem

The *inter-enterprise subsystem* connects enterprise subsystems together when information needs to be shared across geographic or organizational boundaries, such as in a supply chain application. Not all RFID systems contain inter-enterprise subsystems. This section briefly reviews examples of inter-enterprise subsystems and then explains the components necessary to make them operate effectively.

2.5.1 Open System Networks

RFID systems with inter-enterprise subsystems are called *open* or *online* systems because multiple entities have the ability to access tag-related information. In contrast, RFID systems that operate entirely within an enterprise, and thus have no inter-enterprise subsystem, are called *closed* or *offline* systems. The two largest open systems today are the U.S. Department of Defense's Global Transportation Network and Wal-Mart's Retail Link. The DoD and Wal-Mart improve their logistics and operational efficiency by accessing the information in the analytic systems of their suppliers. EPCglobal is building an infrastructure that will enable sharing of RFID data over the Internet by any participating organization. EPCglobal envisions an open system on the scale of the World Wide Web.

To create an open system, each participating organization grants partner organizations access to its analytic systems. The access can occur over a dedicated network for this purpose, a public network such as the Internet, or a VPN that emulates the characteristics of a dedicated network using the infrastructure of a public or shared network. Both dedicated networks and VPNs are sometimes called *extranets*, to denote that information is shared outside the enterprise, as opposed to *intranets*, which are restricted to internal users. To enable extranet access, the implementing organization likely modifies its network firewall to permit RFID-related traffic to traverse the enterprise network boundary and also creates access privileges for external users on the analytic systems themselves. Companies typically sign agreements or memoranda of understanding that describe the roles and responsibilities associated with the access before enabling it.

Figure 2-7 shows how various EPCIS might be connected in an open system network.

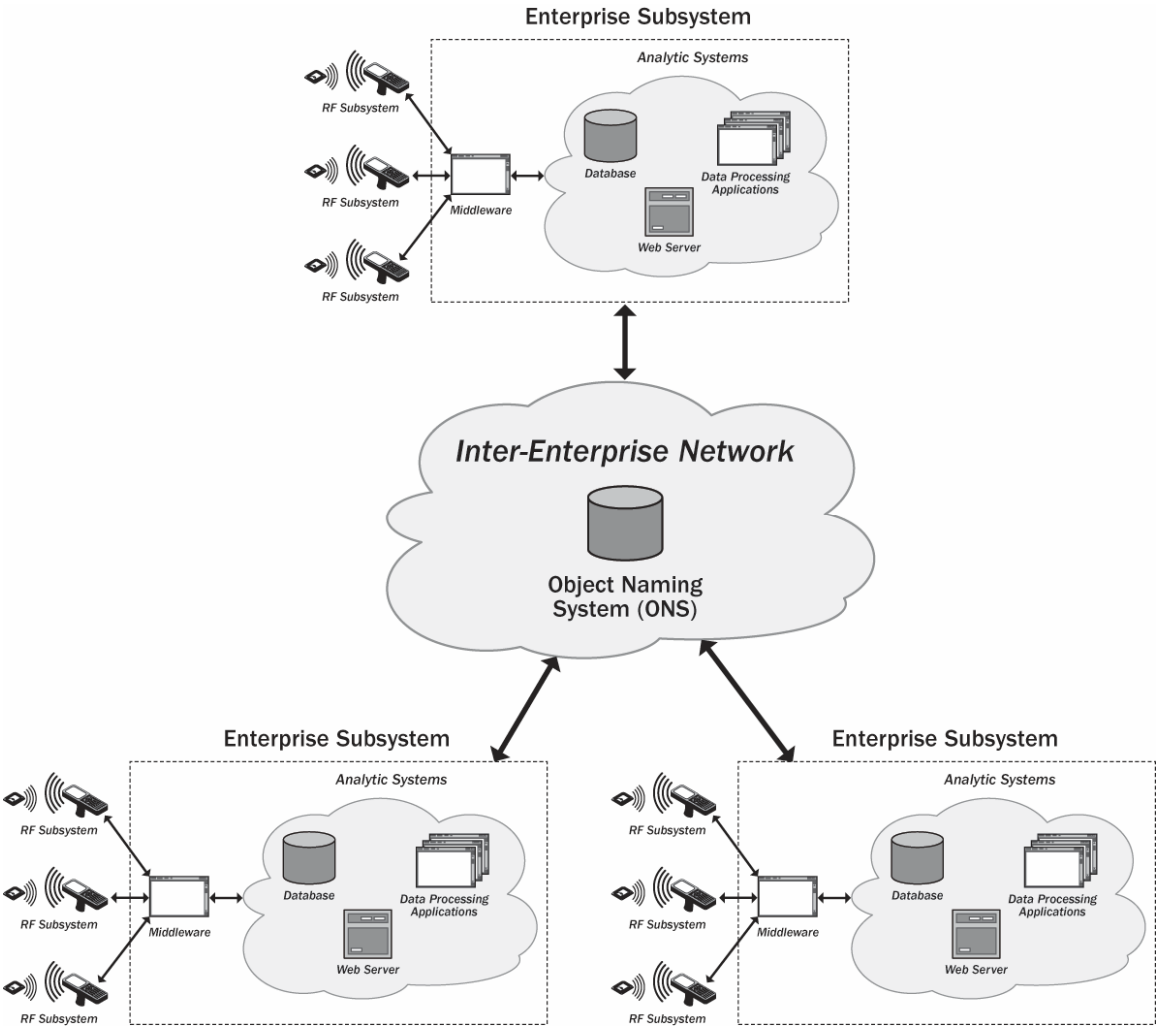

Figure 2-7. Inter-Enterprise Architecture

2.5.2 Object Naming Service (ONS)

Finding information about a tagged object in an open system is a challenge because the information could be located in any one of a number of analytic systems. To solve this problem, EPCglobal created the object naming service (ONS), which is a global distributed database of EPC tag identifiers. Users query the ONS with a particular EPC, and the ONS returns the address information from the EPCIS that contains information associated with that EPC. The user then queries the EPCIS directly to obtain the desired data.

The ONS uses the Internet's Domain Name System (DNS) to support resolution of an EPC with its corresponding EPCIS. ONS EPC resolution works similarly to the name resolution that Internet users employ whenever visiting web sites or sending e-mail messages, but with some significant differences, which are presented in Table 2-2.

Table 2-2. Comparison of Traditional DNS and ONS Resolution Transactions

Traditional DNS	ONS	Discussion
User enters a text-based Uniform Resource Locator (URL) into a Web browser or an e-mail address into a messaging client. Examples: http://www.nist.gov/ john.doe@mail.nist.gov	EPC Uniform Resource Identifier (URI) is converted to a fully qualified domain name. Example: urn:epc:id:sgtin:0513347.004106.325 is converted to: 004106.0513347.sgtin.id.onsepc.com	The EPC is first translated into a form that DNS can interpret. The "root" of the ONS is the domain onsepc.com. ONS is therefore a subset of the Internet DNS.
The messaging client sends the query to a local DNS resolver, which queries a DNS server to resolve the domain name (e.g., www.nist.gov or mail.nist.gov). DNS contains host (A) records for Web servers and other Internet hosts. DNS contains mail exchanger (MX) records for mail servers.	The RFID application forwards the query to a local ONS resolver to resolve the converted URI. The ONS portion of DNS has Naming Authority Pointer (NAPTR) records for EPCs.	The transactions are identical, but they involve different types of records in DNS.
DNS returns an IP address for the relevant server. Example: 129.6.13.23	ONS returns a service registration entry for the relevant EPCIS. Example: http://epcis.nist.gov/epc-wsdl.xml In this example, subsequent communication with epcis.nist.gov occurs using Web Services Description Language (WSDL).	An IP address alone is insufficient for the Web services on which most RFID applications rely. ONS supports several types of service registrations, which define how applications will interact with the EPCIS.
The Web browser or messaging client uses the IP address to contact the server at that address.	The RFID application resolves the domain name in the response using traditional DNS methods and then provides the EPC to the specified service to get information about the tag.	ONS-based RFID applications require additional steps to resolve the service registration.

The EPCglobal ONS is a part of the Internet DNS and therefore is accessible by any Internet user. Some organizations may choose to maintain their own ONS that is not connected to the EPCglobal ONS. Using an independent ONS limits the applications and users that can access it. This characteristic is a beneficial feature for organizations that require their EPCs to remain confidential, but is overly restrictive for organizations that expect large numbers of external users or that cannot anticipate *a priori* who will have a legitimate need for the EPC records (e.g., individual retail consumers seeking support after purchase of a tagged object).

ONS inherits nearly all of the security concerns associated with DNS.[22] Furthermore, security concerns with Web services also apply to EPCIS query systems.[23]

[22] For additional information on DNS security, see NIST SP 800-81, *Secure Domain Name System (DNS) Deployment Guide*, and the Defense Information Systems Agency (DISA) *Domain Name System Security Technical Implementation Guide*, which is located at http://csrc.nist.gov/pcig/STIGs/dns-stig-v3r0.pdf.

[23] For additional information on Web services security, see NIST SP 800-95, *Guide to Web Services Security (DRAFT)*.

2.5.3 Discovery Service

The EPC Discovery Service is similar to ONS because it returns network addresses where data related to an EPC can be found. However, it operates more like a search engine designed to locate records across a range of information sources than a directory service designed to identify a unique authoritative source for each EPC. For instance, EPC Discovery Service can return multiple pointers from multiple organizations, and each organization can provide information about the tagged object at some point in the object's life cycle. More than one EPC Discovery Service can operate in parallel. The various EPC Discovery Services can compete against each other, or they may cater to particular audiences with specific information requirements.

2.6 Summary

RFID is an innovation in AIDC technology that provides significant advantages over earlier technology, such as optical scanning of bar codes. These advantages include the ability to identify objects without optical line of sight over significant distances and the ability to work reliably both indoors and outdoors.

The components of an RFID system can be categorized into three subsystems:

- The RF subsystem,
- The enterprise subsystem, and
- The inter-enterprise subsystem.

Every RFID system includes an RF subsystem, which is composed of (1) tags attached to or embedded in objects and (2) interrogators that read the tags. Important characteristics of tags include their identifier format, the source of their power, the radio frequencies over which they operate, their size and shape, and additional functionality they support, such as security features and connections to environmental sensors. Important characteristics of interrogators include their power output, duty cycle, antenna design, and interface to the enterprise subsystem, which can be either wireless or wired. A wireless enterprise interface enables the interrogator to be mobile. Important aspects of tag-interrogator communication include the singulation protocol, the encoding scheme, and the distance over which tag and interrogator signals can be reliably received.

In many RFID systems, the tags and interrogators are supported by an enterprise system that is composed of middleware, analytic systems, and networking services. The middleware filters data, aggregates data, and manages interrogators and other RFID devices. Analytic systems process and store this information to support business processes. Lastly, the networking services are used to provide the connections among the components of enterprise subsystem and between the enterprise subsystem and the RF subsystem.

RFID systems that share information across organizational boundaries, such as supply chain applications, also have an inter-enterprise subsystem. The RF, enterprise, and inter-enterprise subsystems together allow an RFID system to support business processes. The versatile components of these subsystems allow an RFID system to be tailored to the needs of a particular application. If an inter-enterprise subsystem is constructed to EPCglobal specifications, then it will have an ONS and possibly an EPC Discovery Service. The ONS provides an authoritative lookup for an EPC identifier and returns pointers to the resources from the organization that created that identifier. Finally, EPC Discovery Services serve as a type of search engine for an EPC identifier that can return pointers to multiple organizations that have information related to that EPC identifier.

This page has been left blank intentionally.

3. RFID Applications and Application Requirements

RFID technologies are being deployed by many organizations because they have the potential to improve mission performance and reduce operational costs. To achieve these goals, RFID solutions must be engineered to support the specific business processes that the organization is automating. Applications for RFID technologies are diverse because of the wide range of business processes that exist.

RFID security risks and the controls available to mitigate them are also highly varied. Typically, only a subset of the full range of technologies, risks, and controls is applicable to any given RFID implementation. Important business drivers that shape RFID application requirements and the resulting characteristics of RFID systems include:

- The general functional objective of the RFID technology (i.e., the application type),
- The nature of the information that the RFID system processes or generates,
- The physical and technical environment at the time RFID transactions occur,
- The physical and technical environment before and after RFID transactions take place, and
- The economics of the business process and RFID solution.

This section discusses each of these characteristics in greater detail and provides an overview of common types of RFID applications.

3.1 RFID Application Types

There are many types of RFID applications, of which some of the most common are asset management, asset tracking, automated payment, and supply chain management. The key characteristic differentiating one RFID application from another is the purpose of identifying the tagged items. Table 3-1 lists reasons why an organization might want to identify an item and the general application type that best corresponds to those reasons.

Table 3-1. RFID Application Types

Purpose of Identification	Application Type
Determine the presence of an item	Asset management
Determine the location of an item	Tracking
Ensure affiliated items are not separated	Matching
Correlate information with the item for decision-making	Process control
Authenticate a person (holding a tagged item)	Access control
Conduct a financial transaction	Automated payment

Application types are not mutually exclusive; an implementation can combine elements of several application types. For example, both access control systems and sophisticated asset management systems include tracking features. Supply chain management is a tracking application that spans organizational boundaries and often includes process control and payment transactions.

Personnel responsible for designing and implementing RFID systems should understand what application types apply to their implementation so that they can select appropriate security controls. For example, the security controls needed to protect financial transactions in automated payment systems are different than

those needed for tracking applications. The personnel should also understand that an adversary may leverage RFID technology for an unintended purpose. For example, a warehouse may use RFID technology to determine what items it has in its current inventory, but an adversary may use the same system to track an item's whereabouts after it leaves the warehouse. In this case, an asset management system is later used to enable an unauthorized tracking application, perhaps used by an adversary to locate high value targets or violate personal privacy.

The remainder of Section 3.1 examines each of the application types mentioned in Table 3-1, as well as supply chain management. The section uses hypothetical examples to illustrate the key characteristics of each application type and highlights how they differ from one another. The section also incorporates other examples of each application to provide additional information on current and potential applications of the technology.

3.1.1 Asset Management

RFID-based *asset management systems* are used to manage inventory of any item that can be tagged. Asset management systems using RFID technology offer significant advantages over paper-based or barcode systems, including the ability to access multiple items nearly simultaneously without line of sight or physical contact. These features increase the speed of common asset management tasks, which improves operational efficiency and effectiveness.

Perhaps the simplest form of asset management is Electronic Article Surveillance (EAS), which accounts for items in retail stores.[24] For example, EAS tags are placed on electronic equipment, clothing, books, and many other consumer goods at major retailers. After a customer purchases an item, the sales clerk deactivates the tag. If a person attempts to leave the shop with unpurchased goods, interrogators at the doors will detect the activated tag and trigger an alarm. In this case, the RFID technology determines only one thing: whether or not the EAS tag is still active, indicating that the item has not been properly checked out.

Most RFID-based asset management systems provide additional functionality. For example, at a doctor's office, the medical records clerk can quickly scan the filing system on a monthly or quarterly basis to determine how many medical records are present or missing. The records clerk can also instantly compare the list of missing records with a list of those known to be checked out of the filing system. Without RFID technology, this task could take hours or days to complete by hand. Bar code technology, such as that found at a supermarket, would require physical handling of each medical record, which is labor-intensive.

RFID is also an enabling technology for smart shelves and smart cabinets, which automatically maintain continuous inventories of the items they hold by tracking items entering and leaving. Items are reordered automatically when inventory is low. The smart shelves and cabinets can also be used for theft prevention, alerting personnel when many high-value items are taken at the same time, and perhaps activating a camera to record the event.

3.1.2 Tracking

Tracking applications are used to identify the location of an item, or more accurately, the location of the last interrogator that detected the presence of the tag associated with the item. Many tracking applications are part of an asset management system. One difference between relatively simple asset management systems and tracking systems is that an asset management system can detect the presence of an item with

[24] While EAS can be implemented using RFID technology, it can also be implemented using acoustomagnetic technology. which is not based on RFID. Source: RFID Handbook. Klaus, Finkenzeller..

interrogators at a single location. In contrast, tracking systems require more than one interrogator, as well as a network, so that a central system can aggregate and correlate information received from each of the interrogators.

At transportation hubs (such as ports or train stations), interrogators are placed throughout the facility. The security staff can track the location of its employees wearing RFID-equipped identification badges as they pass through doors or gates. In addition to restricting access to specific areas of the facility, these RFID-enabled identification badges help the security department locate specific staff members during emergency situations and to monitor building evacuations during fire alarms.

Tracking applications can also be used to measure sports performance. Some companies sell systems to track runners and cyclists during races. This application requires each racer to wear a unique tag that is registered with the tracking system. Such systems can be used for any mass start event, including bicycling, running, or triathlons. Different events may require the athletes to wear the tags in a certain way to be detected by the system. For example, runners may be required to put the tag in one of their shoes or cyclists may be required to mount the tag on their bicycles.

3.1.3 Matching

In a *matching application*, two tagged items are matched with each other and a signal (e.g., a light or tone) is triggered if one of the items is later matched with an incorrect tagged item. The most common matching application today occurs in hospitals and involves placing bracelets with tags on mothers and their newborn babies. If a new mother is accidentally given another woman's infant, the system issues an alert. Similar technology allows day care centers to match children to parents or guardians, and hospital patients to their medicines and designated visitors. In the future, RFID tags might match airline passengers with their checked luggage to prevent theft and inadvertent mistakes.

3.1.4 Process Control

Process control applications allow business processes to use information associated with a tag (or the item attached to the tag) to take a customized action. A common process control application is the facilitation of product design variations in manufacturing processes. For example, a tag might be affixed to the frame of a product on an assembly line in a manufacturing plant. The tag's identifier would be associated with desired features of the finished product. At each station in the assembly process, an interrogator would read the tag and take an appropriate action, such as adding a specialized component or using a particular color of paint. In another typical application, machining tools are tagged so that individual tools can be identified by robots and other manufacturing systems.

In asset management, tracking, and matching applications, each interrogator only needed to capture the tag's identifier (a number permanently assigned to the tag) and apply a timestamp to the transaction. In process control applications, additional information beyond the tag's identifier is normally associated with each tag. That information could reside on the tag itself or in a networked database. In either case, the additional information introduces a level of complexity not found in the previously discussed applications. Implementing organizations have additional design issues to consider, such as exactly what information needs to be recorded, where it should be stored, how it should be protected, and their customers' expectation of privacy for that information.

3.1.5 Access Control

Access control systems use RFID to automatically check if an individual is authorized to physically access a facility (e.g., a gated campus or a specific building) or logically access an information technology

system. Some systems are implemented using contactless RFID smart cards instead of mechanical keys. Every individual that is given access to specific areas must carry one of these cards. Locked doors or turnstiles typically protect the areas. To unlock them, authorized personnel must present their smart cards near the appropriate interrogator.[25] The door or turnstile will unlock once the interrogator has authenticated the smart card. The system can be configured such that only certain cards can be used to unlock certain doors or turnstiles.

There are two general types of access control systems: online and offline. Online systems have interrogators that are networked to a central computer. In an online system, each card is linked to a specific person. Each interrogator is supplied by the central computer with a list of individuals that can access the corresponding area. Since this system is networked, the central computer can provide updated access lists to the interrogators. In contrast, offline systems are not networked. In offline systems, the card lists the rooms that the holder can access, perhaps also listing an expiration date. When someone attempts to access a room using the card, the interrogator checks that the card contains one of the permitted identifiers before allowing entry.

RFID technology is also used in automobile key applications, which is effectively a type of access control. There are two basic types: immobilizers[26] and push-button keyless start. With immobilizers, a tag is embedded into a key similar to a traditional vehicle key; the tag in the key is read by an interrogator in the dashboard or steering column. For the key to start the vehicle, it must both have the right shape for the ignition system and contain the tag. Duplication of these keys is significantly more difficult and costly than traditional keys, which has helped to reduce vehicle thefts. The second automobile key application type is push-button keyless start, which allows a driver to start a vehicle without putting a physical key in the ignition. Instead, each driver simply carries a key fob into the vehicle. Once the key fob is detected, the vehicle is started by pushing a start button on the dashboard. This application of RFID can also be used to alert the driver if the key is left in the vehicle or its trunk, helping to prevent accidental lock-outs.

3.1.6 Automated Payment[27]

RFID technology automates a variety of financial transactions, including fare collection on public transit systems,[28] toll collection on roads, fuel charges at gas station pumps, and retail payment using credit cards with embedded RFID tags. The U.S. General Services Administration (GSA) Smart Card Program provides RFID-based cards that support financial transactions.[29] The main advantages over other payment forms are speed and convenience; RFID-based automated payment systems do not require users to physically exchange cash or cards with clerks or machines.

Automated payment systems are a specialized form of access control in which access is granted to credit or debit a financial account. Like other access control systems, they require additional security protections to prevent fraud and abuse. In the case of automated payment, integrity and confidentiality

[25] Different standards for contactless smart cards have different read distances. For example, ISO 10536 close coupling smart cards have a nominal operating range of up to one centimeter and ISO 15693 vicinity coupling smart cards have a nominal range of up to one meter.

[26] Texas Instruments Press Release. Automotive Immobilizer Anti-Theft System Experience Rapid Growth in 1999. June 1, 1999. http://www.ti.com/tiris/docs/news/news_releases/90s/rel06-01-99.shtml

[27] This document does not describe or discuss in detail the multi-layered security controls required for RFID-based automated payment systems. Automated payment systems, point-of-sale systems, and financial transaction systems typically have complex security systems with a variety of controls and safeguards.

[28] Chicago, San Francisco, and Washington, DC use RFID-based fare collection. For additional information see "In Your Pocket: Using Smart Cards for Seamless Travel", October 2004, Katherine Brower, William Henderson. Permanent Citizens Advisory Committee to the MTA.

[29] For additional information on the program, visit http://www.smart.gov/.

controls are needed as well as protection against duplicating or modifying tags; users should not be able to alter debit and credit amounts, and bystanders should not be able to record account numbers or other transaction details. For these reasons, the protocols and cryptography that support automated payment systems typically are considerably more complex than those that support physical access control systems.

Automated payment systems can be online or offline. Online systems, which are the most common, store and process the financial data in a central system networked with the interrogators. Offline systems require the smart card to store "electronic cash" and handle debit and credit transactions, which involve more sophisticated computing and increase the cost of each card. One advantage of offline systems is that they can support the same user anonymity achieved with cash, while centralized systems must link users to their accounts. However, because most users do not demand complete anonymity, the additional complexity and expense of offline systems make them rare.

One example of this technology is currently being used by large resorts and cruise ships. Guests are issued RFID-enabled identification cards upon check-in. These cards are linked to credit card accounts and enable passengers to pay for meals and gift shop items. They are also used for identification when guests disembark the ship or leave the resort grounds.

3.1.7 Supply Chain Management

Supply chain management involves the monitoring and control of products from manufacture to distribution to retail sale. Supply chain management typically bundles several application types, including asset management, tracking, process control, and payment systems. An important distinguishing feature of supply chain management systems is that they span multiple organizations, each of which uses RFID technology that interoperates with the others. When a system is not under one organization's control, it is referred to as an *open* system. The previously discussed systems are *closed* systems because a single organization manages them.[30] Open systems are inherently more vulnerable than closed systems and consequently involve additional security considerations.

Supply chain systems record information about products at every stage in the supply chain. Ideally, tags are affixed to products during the manufacturing process or soon afterward. As a product moves through the supply chain, to the customer, and to post-sale service, the tag's identifier can be used by all supply chain participants to refer to a specific item. In addition, supply chain systems that use active tags can track larger objects such as cargo containers. Tags on these containers can store a manifest of the items shipped in each container. This manifest can be automatically updated when items are removed from the container.

The information collected by a supply chain RFID system offers many benefits. By more accurately tracking products throughout their life cycle, participants can realize improved speed and accuracy of ordering, automated invoicing and payment, fewer supply shortages with lower inventory levels, and reduced *shrinkage* (product loss or theft). Furthermore, RFID-based supply chain systems give management programs better visibility into the supply chain, which enables identification of bottlenecks, targeted recalls, and new forms of market research. Such systems also generate an electronic pedigree for each item. This feature gives buyers evidence of the item's freshness, so they can identify if its useful life has expired. It also provides buyers evidence of a product's authenticity, so buyers can determine if it is an unauthorized clone.

[30] Another common term is a closed *loop* system, which refers to RFID systems that recycle their tags for reuse. Open loop systems could refer to RFID systems that use disposable tags, which is the case in most supply chains.

Large organizations such as the U.S. Department of Defense (DoD) and Wal-Mart are championing RFID-based supply management systems. DoD has mandated that all commodities delivered to any of its distribution centers must be tagged by January 1, 2007.[31]

3.2 RFID Information Characteristics

Once an organization determines the general application type that corresponds to the business process it wants to enhance or enable with RFID technology, it should characterize the information that will be processed by the system. At the low end of the data requirement spectrum is the case of EAS. In EAS, systems, the necessary information is conveyed in a single bit: either the tag is functioning (the item has not yet been sold), or it is has been deactivated (the product has been sold). For this reason, EAS is referred to as a one-bit or single-bit application. Similarly, in the case of relatively simple asset management systems, the only data required is the identifier on the tag. The system merely records which items are present or have been read by the interrogator. Matching applications also have relatively simple data requirements because they just link one identifier with another.

Data requirements increase in tracking applications. The system needs to know which of multiple interrogators last read the tag and at what time. As the tracking systems get more complex, more data is collected, such as changes in the possession of the item (e.g., someone signing for a package) or the particular contents of a container. Process control applications further increase data requirements because they use the recorded specifications of an item to customize actions in the business process.

Supply chain management systems are the most data-intensive RFID application. They not only process data, but they must also maintain information about the data, such as the formats the various organizations in the supply chain use to store and transmit data and the network addresses of database servers that contain data about tagged items.

When determining the appropriate RFID technology and security controls for a given RFID application, the personnel responsible should ask two questions regarding each data element in the RFID system:

- Is it considered sensitive or confidential?
- Does it change, and if so, how frequently?

In many cases, the data element is not sensitive. Organizations need to examine and invest in security controls to protect RFID data depending on the sensitivity level of that data.

Another important characteristic of the data is whether it changes over time. In general, tag identifiers never change, but the data associated with the identifier can change. For example, in asset management applications, the RFID system may maintain information about product features such as make, model, size, color, serial number. These product features typically will be written once and then will not change while the item remains in the system. However, if the asset management application's primary focus is tracking containers rather than specific items, then the data changes frequently as the container is reused to store and transport new items. In access control applications, if a tag acts as a key for a particular item, such as an automobile, then nothing should change once the tag is linked with that item. If the access control application allows a security administrator to change someone's access to different areas and rooms based on changing business roles, then the system must store data related to the access rules.

[31] Radio Frequency Identification (RFID) Policy. Jul 30, 2004. Michael W. Wynne. http://www.acq.osd.mil/log/rfid/Policy/RFID%20Policy%2007-30-2004.pdf

In general, the implementation specifics rather than the application type determine the extent to which data must be modified. When data elements change, the supporting technology must support *write* transactions and must have some form of access control to protect the integrity of the data. When an element does not change, it does not require this support. Organizations planning RFID implementations should analyze what data is required to support the business process and which elements must be modifiable. One important factor is whether tags and their identifiers will be used once and discarded, or reused. The results of this exercise will help organizations identify appropriate RFID technology and security mechanisms to meet their requirements.

3.3 RFID Transaction Environment

The conditions under which interrogators read tags are a significant determinant of an RFID system's technology requirements. The most important parameters regarding the RFID transaction environment include:

- The distance between the interrogator and the tag,
- The amount of time in which a transaction must be completed, and
- Whether or not the interrogator has access to a network and can use the network to store related data.

Sections 3.3.1 through 3.3.3 discuss these parameters.

3.3.1 Distance between Interrogator and Tag

Distance requirements often determine the type of tag that can be deployed. The distance between the interrogator and the tag also has security implications, which are discussed in Section 2.3.3.3. In general, longer distances between the interrogator and the tag could make it easier for an adversary to eavesdrop on their communications. Longer distances also allow an adversary to use its own interrogator to perform unauthorized transactions more easily.

In some cases, the RFID system designer has considerable latitude in setting the distance between interrogator and tag. For example, an application controlling access to a garage might require drivers to place an RFID-enabled badge within inches of an interrogator or it might require a general proximity of several feet to a RFID-enabled transponder within the vehicle. The choice is essentially an application design decision that may include such factors as cost and convenience.

In other cases, the distance between interrogator and tag is dictated by the environment in which the RFID system will be deployed. For example, a tracking application that measures race times at various points on a run may require that interrogators read tags from a distance of several yards. Requiring the participants to locate interrogators and come within a few feet or inches of them would significantly reduce the perceived usefulness of the application to many of its users. In this case, the minimum read distance is a requirement that the RFID solution must meet rather than a choice.

3.3.2 Transaction Speed

Transaction speed can be measured in a variety of ways. A common metric is the number of tags read per second. The main reasons why an application has requirements related to the speed of transactions are:

- Interrogators are expected to communicate with multiple tags nearly simultaneously and cannot do so if each transaction takes longer than a certain period of time.

- Tagged items are in motion and only reside in an interrogator's readable range for a limited period of time.
- The system's users are frustrated if transactions take longer than a short period of time to complete.

For example, in some inventory applications, operators may need to confirm the entire inventory at the end of each business day. In this case, each transaction must complete within a small fraction of a second or the process may take too long to complete. Similar issues may arise when trying to read the tags of multiple guests at the same time at a major event such as the start of a cross-country ski race. In this case, if the transactions take too long, there is a chance that some skiers may go out of range before the interrogator identifies them.

Many security mechanisms introduce latency into RFID transactions. Additional steps are needed to perform authentication, encryption, cover-coding, and other security-related procedures. Each additional step takes time. When considering security controls, organizations need to balance the business impact of each security control's effect on transaction speed with the protection it provides.

3.3.3 Network Connectivity and Data Storage

Whether or not an RFID system's interrogators are networked with database applications has major implications for the architecture of the RFID solution and its security. When an application needs to link data with tags, the data needs to be stored somewhere. If the interrogators are networked with databases, then the data can be stored in the databases. Otherwise, the data must be stored on the tags.

When data is stored centrally on database servers, the tag only needs to contain an identifier, which links the tag to its associated information. In this architecture, the vast majority of the data processing occurs on the supporting systems to which the interrogator is connected. On the other hand, when data is stored on tags, the tags must have some form of memory and support both write and read transactions.

Regardless of where data is stored, the data's integrity must be protected. If the data is sensitive, its confidentiality must also be protected. The methods for achieving this include authentication, access control, and encryption. However, database servers and tags implement these methods in different ways. Nearly all commercial database servers support a wide variety of configurable security controls, but most tags do not. In general, RFID solutions that use networked interrogators to access database servers are preferable to those that store data on tags, both in terms of cost and security. However, a solution may require local storage of data on tags for several reasons, including:

- Extending the network to a remote interrogator is not feasible or is more expensive than using tags that support the required functionality,
- Accessing the data from the network introduces unacceptable latency,
- Network availability is inherently poor, perhaps as a result of harsh operating conditions, which makes accessing data on tags a more reliable approach,
- The participants in an open system have determined that the risk of storing data on tags is less than the risk of opening their networks to external entities, and
- Each tag must collect and store information from a sensor or other data source before it can communicate with a networked interrogator.

3.4 The Tag Environment between Transactions

RFID system requirements depend on what happens between transactions, as well as during transactions. Relevant factors before and after interrogator communication include:

- Whether or not the business process requires that the tag collect data about its environment, and
- The human, technical, and environmental threats that pose risks to the tag's integrity.

These factors are discussed in Sections 3.4.1 and 3.4.2.

3.4.1 Data Collection Requirements

In some applications, each tag is attached to a sensor that stores data in memory that is accessible to the tag. The memory may belong to the sensor, to the tag, or to a combined device. In some cases, the application's core purpose is to capture this data, and RFID technology merely provides a vehicle to access it remotely. In other cases, the sensor data supports an asset management or tracking application, and the objective is to take measurements to ensure that storage or transport conditions are as expected.

3.4.2 Human and Environmental Threats to Tag Integrity

Tags are vulnerable to a variety of threats that could adversely impact the business processes that they support. Selecting appropriate RFID technology and security controls depends on the level of the threat in the environments in which the tags are expected to reside. Some human threats to tags include the ability of an adversary to:

- Damage or destroy a tag,
- Remove the tag from the item to which it was attached,
- Replace a tag with another one, or
- Clone a tag and use the clone for an unintended purpose.

For example, in an EAS application, someone might remove or disable a tag to steal an item from a store without triggering an alarm. Alternatively, someone could replace a tag with one from a lower-priced item before purchasing the tagged item. In an access control application, someone might replace a tag with one that has greater access. If the replaced tag were attached to a picture identification badge, an adversary might be able to effectively gain the privileges of another person while appearing legitimate to personnel who visually check the badge.[32]

Environmental threats to tags include extreme heat, cold, moisture, vibration, shock, and radiation (including sunlight). Any risk assessment of environmental threats should also consider the impact of these conditions to the material to which the tag is attached and the glue or other mechanism that attaches the tag to the item. Impacts of harsh environmental conditions include degradation of tag performance, destruction of the tag, and separation of the tag from its associated item.

Organizations need to assess the likelihood of these threats in their environment and set requirements for their RFID technology accordingly. In general, human threats are more likely to be realized if outsiders

[32] Smartcard standards (as distinguished from RFID standards) include specifications for tamper proofing, including delamination of the cards. Delamination is the removal of a transparent material that, among other things, prevents the easy removal of a tag attached to the surface of the card.

(e.g., customers or members of the general public) have physical access to the tags and therefore the means to engage in malicious behavior. Human threats are also more likely if people have an incentive to perform the attack, such as some form of financial gain or access to a restricted resource.

3.5 RFID Economics

Cost-benefit tests can be applied to any technology project, but RFID systems have differentiating characteristics, especially regarding security. Table 3-2 examines the key factors to consider.

Table 3-2. Economic Factors for Traditional IT Systems Versus RFID Systems

Economic Factor	Traditional Systems	RFID	Discussion
Target of protection	Primarily, the information that the system stores and processes. Secondarily, the hardware and software components of the system.	In asset management and tracking systems, organizations typically are more concerned with protecting the item being tagged (especially against theft) than the information that the system processes. Similarly, in RFID-based access control systems, the ultimate objective typically is protecting physical assets rather than information.	The value of the information and physical assets is entirely dependent on the specific implementation. In general, it is easier to place a value on physical assets than information assets because physical assets have a known price and depreciation schedule.
Number of units	Systems can involve anything from a handful to several thousand users and components; only the very largest IT systems exceed this scale.	Small-scale RFID applications typically are not economical. RFID systems can involve from hundreds to millions of tags.	In implementations with many RFID tags, small changes in the unit cost of tags (e.g., several cents a tag) can have enormous impacts on the total cost of the solution and, therefore, its economic feasibility. Small changes in the unit costs of traditional IT system components typically do not impact the economic viability of the implementation.
First (or upfront) cost of security functionality	Basic security functionality (e.g., authentication and encryption) usually is bundled into commercial-off-the-shelf operating systems, database software, and network components; it does not increase the upfront cost of the system from the consumer's perspective.	Incorporating basic security functionality significantly increases the cost of a tag. Encryption that is commonly supported on traditional IT systems is currently cost-prohibitive on tags for most applications.	The upfront cost associated with security functionality likely is a more significant factor in RFID procurement decisions than it is for traditional IT systems.
Operational complexity and cost of basic security controls	While costs can vary greatly, many controls such as passwords are commonplace and are not perceived as unnecessarily burdensome. Many enterprises require users to have complex unique passwords that change at least every 90 days.	Assigning unique tag passwords or periodically changing tag passwords may be administratively unmanageable in many RFID applications.	The operational costs of even basic security controls such as passwords need to be carefully considered when setting policy for and designing an RFID implementation.

3.6 Summary

RFID technology can support a wide range of applications—from asset management and tracking to access control and automated payment. The business requirements for these applications are as varied as the applications themselves. In particular, they are implementation-specific and depend on such factors as:

- The nature of the information that the RFID system manages, including its sensitivity and how it changes over time,
- The RFID transaction environment, including the distance between interrogator and tag, the required speed of the transactions, and the level of network connectivity during the transaction,
- The characteristics of the tag environment between transactions, such as whether tags collect data from sensors and the human and environmental threats that tags face, and
- The economics of RFID technology and security controls.

This page has been left blank intentionally.

4. RFID Risks

RFID technology enables an organization to significantly change its business processes to:

- Increase its efficiency, which results in lower costs,
- Increase its effectiveness, which improves mission performance and makes the implementing organization more resilient and better able to assign accountability, and
- Respond to customer requirements to use RFID technology to support supply chains and other applications.

The RFID technology itself is complex, combining a number of different computing and communications technologies to achieve the desired objectives. Unfortunately, both change and complexity generate risk. For RFID implementations to be successful, organizations need to effectively manage that risk, which requires an understanding of its sources and its potential characteristics.

This section reviews the major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments. The risks are as follows:

- **Business Process Risk.** Direct attacks on RFID system components potentially could undermine the business processes the RFID system was designed to enable.
- **Business Intelligence Risk.** An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.
- **Privacy Risk.** The misuse of RFID technology could violate personal privacy when the RFID application calls for personally identifiable information to be stored on or associated with a tag. The personal possession of functioning tags also is a privacy risk because it could enable tracking of those holding tagged items.
- **Externality Risk.** RFID technology potentially could represent a threat to non-RFID networked or collocated systems, assets, and people.

An important characteristic of RFID that impacts all of these risks is that RF communication is invisible to operators and users. In other AIDC and IT systems it often is easier to identify when unauthorized behavior is occurring. This section characterizes the risks listed above in more detail. The security controls that mitigate these risks are discussed in Section 5.

4.1 Business Process Risk

RFID systems typically are implemented to replace or enhance a paper or partially automated process. Organizations implementing RFID systems could become reliant on those systems, which if not implemented properly might be less resilient to disruptions than the systems they replace. For example, suppose that a warehouse replaces its paper-based inventory management system with an RFID-enabled system. The paper system involves storing completed forms at the warehouse and sending form duplicates to a central office, while the new RFID system locates its backend database servers at a single computing center. In this environment, the paper system might be more resilient to a local disaster than the RFID system, despite the increased efficiency or effectiveness of the RFID-enabled business process.

Failure in any component or subsystem of the RFID solution could result in system wide failure. In the warehouse example, system wide failure might result from many causes, such as loss of the network connection between the warehouse and the computing facility, a software virus that disables critical middleware functionality, or a new source of radio inference that prevents interrogators from accurately reading tags. If an RFID system is rendered unavailable for any reason, then potential impacts can range from a deceleration of the business process to the loss of critical business or operational records. If the system is mission critical, then the consequences could be devastating to the organization's performance.

Table 4-1 reviews some of the factors that determine the level of business process risk.

Table 4-1. Factors Influencing Business Process Risk

Factor	Discussion
The importance of the RFID-supported business processes to the mission of the organization	The tighter the link between the RFID-supported business process and the mission of the organization, the greater the impact will be if the business process is degraded or disabled. Organizations whose core business is logistics or asset management stand the most to lose when their supporting RFID systems fail. If an organization's primary mission is outside these areas, it is less likely to be impacted. For example, a hospital whose primary mission is patient care could be significantly inconvenienced with the loss of an RFID system, but medical care is likely to continue regardless of the system's status.
The robustness of business continuity planning or fallback procedures that can be implemented when the RFID system is unavailable	In many applications, the fallback procedure is trivial to implement, in which case business process risk is relatively low. For example, a push-button keyless start automobile key could be designed to operate as a physical key when the RFID system is not functioning properly. If an RFID-based automated payment system is down, cash and credit cards are viable alternatives. In many cases, bar codes or visual inspection of tagged items may provide a workable interim solution until the RFID system returns to operation. In general, as the complexity of the system increases, so does the risk and, consequently, the need for business continuity planning. Plans should include the ability to use geographically distributed personnel and enterprise equipment so that timely recovery is possible in case of local disasters.
The environment in which the RFID technology is located	Important environment factors include the existence of radio frequency interference, electrostatic discharge, vibration, abrasion, extreme temperatures, or humidity. The presence of physical access controls also is a key determinant of the risk to business processes from human threats. Public and densely populated areas pose more risk than tightly controlled or remote areas.
The existence of adversaries with the motivation and the capability to perform RFID attacks	Individuals or groups with malicious intent are more likely to target organizations with a high public profile, such as government agencies, than less well-known entities. Individuals seeking financial gain are likely to target RFID systems that support financial transactions, those that contain sensitive information on individuals, and systems that involve high-value assets. The computer attacker seeking a challenge is also a threat for all systems. Individuals may try to replace the tag on a high value item in a retail store with a tag from a low value item to purchase the high value item at a reduced cost.
The presence and effectiveness of RFID security controls	The stronger the controls and countermeasures, the lower the risk. These are discussed in more detail in Section 5.

Unlike most of the other risks, business process risk can occur as a result of both human action and natural causes. Moreover, human causes may be intentional or unintentional. For example, a tag might

fail to perform its intended function because someone removed it from its packaging, an employee accidentally damaged it with a box cutter, or a severe storm covered it in ice.

An example of an intentional attack on an RFID business process is cloning, which occurs when an adversary reads information from a legitimate RFID tag and then programs another tag or device to emulate the behavior of the legitimate tag. Documented examples of cloning have occurred in tags used for financial payment[33] and access control.[34] Another attack on an RFID business process would be removing a tag from the item it is intended to identify and attaching it to another unrelated item.

Potential problems are not just limited to the RF subsystem. If the network supporting the RFID system is down, then the RFID system is likely down as well. In supply chain applications, network failures at any point in the chain have the potential to impact the business processes of any subsequent link in the chain. For example, if a supplier is unable to write manifest data to a tag, then the recipient cannot use that data in its operations even if its RFID interrogators and network infrastructure are fully functional. Servers hosting RFID middleware, databases, analytic systems, and authentication services are all points of failure. Any efforts to assess business process risk need to be comprehensive, because such a wide variety of potential threats exist. All of these threats have the potential to undermine the supported business process and therefore the mission of the implementing organization.

4.2 Business Intelligence Risk

RFID is a powerful technology, in part, because it supports easy access to information about assets and people that either previously did not exist or was difficult to create or dynamically maintain. While this easy access is a significant benefit, it also represents a substantial risk because unauthorized parties potentially could have the same easy access to that information if proper controls are not in place. This risk is distinct from the business process risk because it can be realized even when business processes are functioning as intended.

A competitor or adversary can gain information from the RFID system in a number of ways, including eavesdropping on RF links between interrogators and tags, performing independent queries on tags to obtain relevant data, and obtaining unauthorized access to a back-end database storing information about tagged items. Supply chain applications may be particularly vulnerable to this risk because a variety of external entities may have read access to the tags or related databases. The risk of unauthorized access is realized when the entity engaging in the unauthorized behavior does something harmful with that information.

In some cases, the information may trigger an immediate response. For example, someone might use an interrogator to determine whether a shipping container holds expensive electronic equipment, and then break into the container when it gets a positive reading. Similarly, someone seeking to cause damage might attempt to destroy a target if RFID technology can determine that the vehicle is carrying hazardous materials. These scenarios are examples of *targeting*.

In other cases, data might also be aggregated over time to provide intelligence regarding an organization's operations, business strategy, or proprietary methods. For instance, an organization could monitor the number of tags entering a facility to provide a reasonable indication of its business growth or operating practices. In this case, if someone determined that a warehouse recently received a number of very large

[33] Researchers from the Johns Hopkins University and RSA Laboratories cloned tags used as vehicle immobilizers and electronic payment tokens. Source: http://rfidanalysis.org/

[34] A University of Waterloo student cloned a proximity card used for access control. Source: RFID Applications, Security, and Privacy. 2006. pg. 291-301.

orders, then that might trigger an action in financial markets or prompt a competitor to change its prices or production schedule.

Table 4-2 reviews some of the factors that determine the level of business intelligence risk.

Table 4-2. Factors Influencing Business Intelligence Risk

Factor	Discussion
The type of information stored on the tag	If tags contain nothing more than identifiers, then the risk is substantially lower than it would be if tags store data about the tagged item. However, some adversaries could obtain valuable intelligence from the mere existence of a tag (e.g., someone is present at particular location) or the number of tags at a particular location (e.g., a certain level of inventory is available).
The existence of adversaries with the motivation and the capability to perform RFID attacks	For an attack to be successful, the attacker must have the knowledge and tools necessary to perform the attack and a motive for engaging in malicious behavior. Many organizations have known adversaries and consequently need to implement active countermeasures against that threat. Other organizations may not have identifiable adversaries with the required characteristics. However, organizations should proceed with caution because they may not be able to anticipate who may be an adversary in the future. For example, disgruntled employees always represent an insider threat even if the organization has not experienced attacks to date.
The usefulness or relevance of information available to the adversary	The most critical item is what information is stored on tags. With the exception of some access control applications, if tags contain nothing more than identifiers, then the risk is substantially lower than it would be if tags store data about the tagged item. When information beyond an identifier is stored on tags, it could be a rich source of information of data such as personal records, location history, container manifests, and sensor measurements. Some adversaries might obtain valuable intelligence from the mere existence of a tag or knowledge of the number of tags at a particular location. For example, if the tagged item is associated with an individual, then it could reveal the location of that person. Accordingly, organizations need to consider how an adversary might use information about the presence of a tag as well as data stored on the tag.
The location of RFID components	If tagged items are located in public areas, business intelligence risk is considerably higher than it would be if tags stay within access-controlled facilities. Another consideration is the ability of radio communication to occur beyond the physical perimeter. For example, if an adversary can read tags outside of a facility's fence, then the business intelligence risk is higher than it would be if signals were limited to a few feet and could not easily penetrate walls. The physical location of supporting IT infrastructure can also play a role in risk determination.
The presence and effectiveness of RFID security controls	The use of controls such as database access controls, password-protection, and cryptography can significantly mitigate business intelligence risk if applied properly. Section 5 discusses these controls in more detail.

4.3 Privacy Risk

RFID technology raises several important privacy concerns. One concern is that organizations that are implementing RFID systems to serve particular business processes might not be sensitive to how the RFID information could be used for unintended purposes. In many cases, the alternative uses of the information might be of no interest to the organization implementing the RFID technology, which means it may have no incentive to effectively control those uses unless required by law or policy. This

distinguishes the privacy risk from the previous risks, in which the implementing organization has strong incentives to manage the risk regardless of legal or policy requirements.

For example, if a consumer purchases a tagged clothing item and the tag is not disabled or removed after purchase, then the seller or another organization could later use the existence of the tag on the person's clothing to track the location of that individual, albeit in a limited physical range. The tag's presence may also reveal the personal preferences of the individual, such as where they shop or what brands they buy. Several technologies exist to prevent revelation of personal information,[35] but nonetheless such scenarios are possible. Implementing organizations need to do what they can to prevent them.

In this case, the actual privacy risk is borne by the consumer, not the retail sales organization that implemented the RFID solution. Nevertheless, the implementing organization still has related risks, including:

- Consumers could avoid or boycott the store because of real or perceived privacy concerns about RFID technology,
- The organization might be held legally liable for any consequences of the weak privacy protections, and
- Employees, shareholders and other stakeholders could disassociate with the organization due to concerns about corporate social responsibility.

Some factors that impact the level of privacy risk include:

- Storage of personal information on tags,
- The ability of tags to be disabled after their use in a business process has been completed,
- The ability of users to effectively shield tags to prevent unauthorized read transactions, and
- The effectiveness of security controls on RFID databases and other components.

Privacy laws dictate responsibilities for Federal government agencies and for companies in certain industries, such as financial and health care. For example, Federal agencies must develop privacy impact statements for all of their major information systems, which would include RFID systems. A detailed discussion of privacy policy is beyond the scope of this guide, but privacy issues are still deeply intertwined with RFID security issues. In some cases, technologies that enhance personal privacy pose some level of risks to business processes. At the same time, many of the security controls to mitigate other risks also strengthen privacy protections. In particular, most efforts to ensure the confidentiality of RFID data, even if focused on the needs of the implementing organization, also serve the interests of personal privacy. For additional information on privacy concerns, see Section 6.

4.4 Externality Risk

RFID systems typically are not isolated from other systems and assets in the enterprise. Every connection point between the RFID system and something outside the RFID system represents a potential vulnerability for the entity on the other side of the connection, whether that is an application process, a valued asset, or a person. Externality risks are present for both the RF and enterprise subsystems of an RFID solution. The main externality risk for the RF subsystem is hazards resulting from electromagnetic

[35] For example, the EPC *kill* command disables the ability of interrogator to subsequently read data on the tag. The *kill* command is discussed in more detail in Section 5.3.1.1.

radiation, which can range from adverse human health effects[36] to ignition of combustible material, such as fuel or ordnance. The main externality risk for the enterprise subsystem is successful computer network attacks on networked devices and applications. Computer network attacks can involve malware (e.g., worms and viruses) or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage. The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application.

Because the externality risk by definition involves risks outside of the RFID system, it is distinct from both the business process and business intelligence risks; externality risks can be realized without having any effect on RFID-supported business processes or without revealing any information to adversaries.

4.4.1 Hazards of Electromagnetic Radiation

The four most prominent types of hazards from electromagnetic radiation are as follows:

- **Hazards of electromagnetic radiation to ordnance (HERO).** There is a risk that ordnance will be detonated by the electromagnetic radiation that RFID systems use to communicate. U.S. military regulations require RF systems to be HERO evaluated.[37]
- **Hazards of electromagnetic radiation to fuel (HERF).** There is a danger of electromagnetic waves causing sparking or arcing between two metals, which could ignite fuel or other volatile substances.
- **Hazards of electromagnetic radiation to people (HERP).** Electromagnetic waves can thermally heat living tissue. Humans have no internal sensation of heat and accordingly cannot feel this heating when it occurs. The eyes and testes are at greatest risk from this hazard because these areas of the body have lower blood flow and dissipate heat more slowly.[38] In addition, electromagnetic radiation has the potential to affect humans by interfering with medical devices (e.g., hearing aids and implantable defibrillators).[39]
- **Hazards of electromagnetic radiation to other materials**. Electromagnetic radiation could be hazardous to other substances such as blood products, vaccines, and pharmaceuticals, although research on the potential impact of RFID operations on these substances is not conclusive.

While each category has special characteristics, the sources of the threat and mitigating controls are similar across all of them. Table 4-3 reviews some of the factors that determine the level of the electromagnetic radiation risk. For additional information on hazards of electromagnetic radiation, see Appendix D.

---

[36] In addition, the US Food and Drug Administration has identified the potential for human implanted RFID chips to be incompatible with magnetic resonance imaging (MRI). Source: http://www.sec.gov/Archives/edgar/data/924642/000106880004000587/ex99p2.txt

[37] DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," September 8, 2004.

[38] Federal Communications Commission. Office of Engineering and Technology. OET Bulletin 56. Fourth Edition. August 1999. p. 6-7.

[39] While RF interference with pacemakers is a concern, it does not appear to pose a serious problem in practice. .Federal Communications Commission. Office of Engineering and Technology. OET Bulletin 56. Fourth Edition. August 1999. pp. 26.

Table 4-3. Factors Influencing Electromagnetic Radiation Hazards

Factor	Discussion
RFID operating power and frequency	The likelihood of a hazard is related to the operating power at a specific frequency. The greater the power, the greater the probability of an adverse effect. For reference, UHF RFID readers in the United States can output up to 4 watts of power.[40] However, RFID equipment may inadvertently be operating at a higher power than the equipment power rating specification. Organizations with this concern could conduct a pilot study and measure the output power to ensure that their RFID equipment is transmitting at its expected power level. The greatest hazard to humans is caused by electromagnetic radiation in the very high frequency (VHF) band between 80 and 100 MHz. Depending on the size, shape, and height of a person, a specific frequency in this band causes maximum heating. In comparison, microwave ovens operate near a resonance frequency of water (i.e., 2.450 GHz).[41]
Distance between RF subsystem components (i.e., tag and interrogator) and object of concern	The closer the object of concern is to the source of the radiation, the greater the likelihood of an adverse effect. The strength of the signal declines sharply as the distance from the transmitter increases[42], which means that relatively small differences in distance may have relatively significant implications for relevant hazards.
Complex cavity effects	Signal reflections and other electromagnetic effects can focus radiation in unintended ways. Metal items, including doors, window frames, and furniture, can reflect, diffract, and scatter electromagnetic radiation.

4.4.2 Computer Network Attacks

RFID technology represents a new attack vector on an enterprise network. Once RFID systems are implemented, a possibility exists that attackers could reach non-RFID and enterprise subsystem computers through an interrogator, although no such attack is known to have successfully occurred to date. If the system involves wireless handheld interrogators, then the wireless link between the interrogator and the networked middleware servers is another point of entry. Once RFID servers are compromised, they can be used to launch attacks on other networked systems. Attack possibilities include the introduction of malware (e.g., a worm or virus) or the exploits of a single adversary compromising one computer at a time. Once additional systems are compromised, all types of adverse consequences to the IT infrastructure are possible, including loss of confidentiality, integrity, and availability.

While the risk of network compromise through an RFID interface is considered low, the history of computer and network security suggests that such a breach is inevitable, especially as RFID technology proliferates. RFID air-interface protocols do not support the execution of remote commands on the RFID interface, but conceivably an adversary could exploit a buffer overflow vulnerability on an interrogator by sending it data in formats outside those expected by the protocol. In some cases, this could enable the adversary to insert code or commands in memory buffers read by privileged processes. The potential consequence is that the adversary could gain full control of the device and use that control to attack other systems.

[40] FCC Part 15 Section 247

[41] Federal Communications Commission. Office of Engineering and Technology. OET Bulletin 56. Fourth Edition. August 1999. pp. 7.

[42] In the near field, the power of the signal is proportional to $1/d^3$ and in the far field, the power of the signal is proportional to $1/d^2$ where d represents the distance between interrogator and tag.

This type of attack was shown to be possible by RFID security specialists using RFID viruses.[43] An RFID virus is a small program or malware encoded on a tag that becomes active once it has been read and is then passed to the middleware or database of an IT system. The virus can take advantage of internal software weaknesses in the middleware or database products and has the ability to replicate itself to other tags. This risk is not unique to RFID as a virus or malware can also be introduced via other AIDC data carriers (e.g., two dimensional bar codes). RFID software designers are aware that this is a data validation issue and that software components must be designed and developed using secure software development practices.

Some factors influencing the magnitude of the risk to the IT infrastructure and the applications they support are presented in Table 4-4.

Table 4-4. Factors Influencing the Cyber Attack Risk

Factor	Discussion
Level of network connectivity	The greatest factor determining the risk from an RFID system is the number and value of the systems with which it interconnects. Each host represents both a potential source of and target of attacks. If external network access is limited, risk is limited as well.
Vulnerability of RFID software	The ability of RFID components to be breached largely depends on the assurance of the implementing software (e.g., interrogator drivers, middleware, analytic systems). Poorly developed software might be more easily compromised.
Physical proximity to RF subsystem	The likelihood that an adversary with both the skills and motivation to compromise RF subsystem components depends heavily on whether the adversary is able to get within reasonable proximity to the components so that RF communication is possible. When tags and interrogators are in public or easily accessible spaces, greater risk exists than when they are not in these areas. However, RFID enterprise servers can still be breached from network-based attacks even if the attacker has no access to RF subsystem components.
Presence and effectiveness of security controls	Known, effective, and widely available strategies exist for preventing or limiting the impact of most computer network attacks. However, these strategies are only effective if they are implemented properly. Security controls are discussed in more detail in Section 5.

4.5 Summary

For RFID implementations to be successful, organizations should effectively manage their risk. The major categories of risk are as follows:

- **Business Process Risk.** This encompasses threats and vulnerabilities that could cause part or all of the RFID system to fail. Potential impacts range from a deceleration of the business process to the loss of critical business or operational records. If the system is mission-critical, the consequences could be harmful to the organization's performance. Business process risk can occur for many reasons, including human action (either benign or malicious) and natural causes. Any efforts to assess business process risk need to be comprehensive, because such a wide variety of potential threats exists. All of these threats have the potential to undermine the supported business process and therefore the mission of the implementing organization.

[43] M. Rieback, B. Crispo and A.S. Tanenbaum, "Is Your Cat Infected with a Computer Virus?," in the proceedings of PerCom 06: 4th Annual IEEE International Conference on Pervasive Computing and Communications, 13-17 March 2006.

- **Business Intelligence Risk.** This involves threats and vulnerabilities that could permit unauthorized parties to gain access to information. A competitor or adversary can gain information from the RFID system in a number of ways; supply chain applications are often particularly vulnerable because external entities may have read access to tags or related databases. The risk of unauthorized access is realized when the entity engaging in the unauthorized behavior does something harmful with that information. In some cases, the information may trigger an immediate response, such as breaking into a container holding valuable goods. In other cases, data may also be aggregated over time to provide intelligence regarding an organization's operations, business strategy, or proprietary methods.

- **Privacy Risk.** An organization's RFID tag information could be used by others to violate the privacy of the parties (i.e., consumers) that are in possession of the tagged items. In this case, the actual privacy risk is borne by the consumer, not the organization that implemented the RFID solution. Nevertheless, the implementing organization still has risks, primarily the reaction and response from consumers, employees, government officials, investors, and others.

- **Externality Risk.** Every connection point between an RFID system and other systems represents a potential vulnerability. The main externality risk for an RF subsystem is hazards resulting from electromagnetic radiation, which can range from adverse human health effects to ignition of combustible material, such as fuel or ordnance. The main externality risk for an enterprise subsystem is successful attacks on networked hosts and applications. Computer network attacks can involve malware or attack tools that exploit software vulnerabilities and configuration weaknesses to gain access to systems, perform a denial of service, or cause other damage. The impact of computer network attacks can range from performance degradation to complete compromise of a mission-critical application.

This page has been left blank intentionally.

5. RFID Security Controls

This section discusses security controls that can potentially mitigate the business risks associated with RFID systems. As previously discussed, RFID implementations are highly customized. As a result, the security controls listed are not all applicable or effective for all RFID applications. Organizations need to assess the risks they face and choose an appropriate mix of controls for their environments, taking into account factors such as regulatory requirements, the magnitude of the threat, and cost and performance. This section covers security controls applicable to most RFID implementations. It does not address the security of RFID-enabled smart cards and payment systems.

This section also does not discuss security controls related to general IT systems, such as network infrastructure, databases, and web servers because these are already covered by other security requirements and guidance. For example, EPC Information Service (EPCIS) servers, which can be accessed by trading partners through the Internet, should be protected by the same types of controls that would be used for any other Internet-facing system (e.g., encryption of sensitive communications, access control to prevent unauthorized access to data and systems) to ensure the security of the data collected by the RFID system. Guidance on topics such as IT server, application, database, or network security is available from many sources, including NIST's Computer Security Resource Center (CSRC).[44]

The RFID security controls discussed in this section are divided into three groups:[45]

- **Management.** A management control involves oversight of the security of the RFID system. For example, the management of an organization might need to update existing policies to address RFID implementations, such as security controls needed for an RF subsystem.
- **Operational.** An operational control involves the actions performed on a daily basis by the system's users. For example, RFID systems need operational controls that ensure the physical security of the systems and their correct use.
- **Technical.** A technical control uses technology to monitor or restrict the actions that can be performed within the system. RFID systems need technical controls for several reasons such as protecting data on tags, causing tags to self-destruct, and protecting wireless communications.

The information provided for each control includes:

- A description of the control and how it works,
- The types of implementations or applications where the control might be helpful,
- The benefits that the control provides, such as which risks it mitigates, and
- The weaknesses of the control, including why it might not be effective in some environments, and what residual risks and other concerns remain even if the control is implemented.

The summary at the end of Section 5 summarizes the controls and maps them to the risk categories discussed in Section 4.

---

[44] The CSRC is located at http://csrc.nist.gov/publications/nistpubs/index.html. Appendix D contains a list of NIST publications that address general security issues and provide guidance for the configuration of specific technologies that might be of use when securing an RFID system, including the computing devices in the enterprise subsystem.

[45] More information on security controls is available in NIST SP 800-53.

5.1 Management Controls

Management personnel usually need to include RFID technologies as part of the IT infrastructure being managed. For example, if existing policy prohibits wireless technology, then it would need to be amended to permit wireless use for RFID components only. Management is also typically involved in risk assessment, system planning, system acquisition, as well as security certifications, accreditations, and assessments. The sub-sections below discuss management controls for RFID systems in more detail.

5.1.1 RFID Usage Policy

Control: An RFID usage policy describes the authorized and unauthorized uses of RFID technology in an organization and the personnel roles assigned to particular RFID system tasks. The usage policy should be consistent or integrated with the organization's privacy policy, which addresses topics such as how personal information is stored and shared. Additional information resources are found in the privacy guidance in Section 6.

Applicability: All organizations that use RFID technologies or are considering using them.

Benefits: The policy establishes the framework for many other security controls. It provides a vehicle for management to communicate its expectations regarding the RFID system and its security. It enables management to take legal or disciplinary action against individuals or entities that do not comply with the policy.

Weaknesses: The existence of a policy does not ensure compliance with the policy. A policy needs to be coupled with the implementation and enforcement of appropriate operational and technical controls to be effective.

5.1.2 IT Security Policies

Control: IT security policies describe the approach to achieve high-level security objectives of the usage policy. The IT policies related to RFID should cover each RFID subsystem and not just the RF subsystem. IT security policies for RFID systems should address:

- Access control to RFID information, especially records contained in RFID analytic system databases,
- Perimeter protection, including port and protocol restrictions for network traffic between the RF and enterprise subsystems and between the enterprise subsystem and a public network or extranet,
- Password management, particularly with respect to tags' access, *lock*, and *kill* passwords,
- Management system security for interrogators and middleware, including the use and protection of SNMP read and write community strings,[46]
- RFID security training for system administrators and operators, and
- Management of associated cryptographic systems, including certification authorities and key management.

[46] *SNMP community strings* are passwords that provide anyone with an SNMP management client and network access the ability to manage the associated systems. Knowledge of the *read community string* provides the holder the ability to view the system configuration and track system behavior. Knowledge of the *write community string* provides the holder the ability to reconfigure system components.

Applicability: All RFID implementations, particularly those with enterprise subsystems or inter-enterprise subsystems.

Benefits: Well-crafted security policies govern the mitigation of business risks associated with the use of RFID technologies. The policies provide requirements and guidance for the individuals designing, implementing, using, and maintaining RFID systems. For example, IT policies help the personnel designing RFID systems or procuring system components to make appropriate decisions. Similarly, they help system administrators correctly implement and configure software and related network components.

Weaknesses: The existence of a policy does not ensure compliance with the policy. A policy needs to be coupled with the implementation and enforcement of appropriate operational and technical controls to be effective.

5.1.3 Agreements with External Organizations

Control: When data associated with an RFID system needs to be shared across organizational boundaries formal agreements among the participating organizations can codify the roles and responsibilities, and in some cases the legal liability, of each organization. These formal agreements are usually documented as a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU). The MOU or MOA specifies the network connections and authentication mechanisms to be used, the data to be shared, and the manner in which data should be protected both in transit and at rest. It may also address controls on vendors, subcontractors, and other third parties to the extent they have access to the system.[47]

Applicability: Any RFID system involving more than one organization, which is most common in supply chain applications.

Benefits: Having an MOA or MOU significantly reduces the potential for subsequent misunderstandings and security breaches. They enable signatories to communicate their respective security requirements while also realizing the benefits of the business partnership that led them to collaborate in the development and use of the RFID system.

Weaknesses: Monitoring an external organization's enforcement of an agreement is difficult without full access to its systems and personnel, which is highly unlikely. As a result, violations may occur without detection. This risk can be mitigated with independent audits if signatories agree to hire third-parties to conduct such audits.

5.1.4 Minimizing Sensitive Data Stored on Tags

Control: Instead of placing sensitive data on tags, the data could be stored in a secure enterprise subsystem and retrieved using the tag's unique identifier.

Applicability: Applications that use tags with on-board memory.

Benefits: Adversaries cannot obtain information from the tag through rogue scanning or eavesdropping. Organizations can more cost-effectively perform data encryption and access control in the enterprise subsystem than in the RF subsystem.

[47] For additional information on agreements with external organizations, see NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, which can be found at http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf.

Weaknesses: Adversaries can often obtain valuable information from the identifier alone. For example, knowledge of the Domain Manager and Object Class bits of an EPC tag may reveal the make and model of a tagged object concealed in a container. An adversary might target containers based on the perceived worth of their contents. Also, placing data in the enterprise subsystem makes the availability of that data contingent on the availability of the network. Retrieving data over a network also introduces a small delay, which could be unacceptable for some applications. Section 3.3.3 discusses why organizations might choose to store data on tags even after taking into consideration the risks of doing so.

5.2 Operational Controls

There are several types of operational controls. For instance, physical access controls restrict access to authorized personnel where the RFID systems are deployed. Another operational control is the proper placement of RF equipment to avoid interference and hazards from electromagnetic radiation. Organizations can destroy tags after they are no longer useful to prevent adversaries from gaining access to their data. Another control is implementing operator training so that staff using the system follow appropriate guidelines and policies. Existing operational controls might also need to be extended to include the RFID system. For example, network security controls might need to be changed so that they permit authorized use of the RFID system and prevent unauthorized network connections to its components. Data that is written to tags can be backed up on the enterprise subsystem in case the tags are lost or destroyed, and the enterprise subsystem can also be backed up regularly in case of subsystem failure. The sub-sections below discuss operational controls for RFID systems in more detail.

5.2.1 Physical Access Control

Control: Physical access controls include fences, gates, walls, locked doors, turnstiles, surveillance cameras, and security guards. When the objective is to limit radio communication over a short distance, room walls or partitioned stalls might provide adequate protection if they are opaque to the relevant radio frequencies that the RF subsystem uses.

Applicability: All RFID implementations except those in which RFID tags or other system components are in public areas.

Benefits: Physical access controls limit the ability of an adversary to get close enough to RFID system components to compromise RFID data security or to modify, damage, or steal RFID system components. Physical security applies to all RFID subsystems. In the RF subsystem, the primary objective of the control is to prevent unauthorized or hazardous radio communications. In the enterprise and inter-enterprise subsystems, the primary objective is to prevent physical access to system components. Examples of risks that are mitigated by physical access controls include:

- Unauthorized reading and writing of tag data,
- Rogue and cloned tags,
- Interrogator spoofing,
- Denial of service resulting from radio interference or unauthorized commands,
- Targeting,
- Physical destruction of RFID equipment, and
- HERF/HERO/HERP.

Weaknesses: This control has several potential weaknesses, including:

- Physical access controls are not a countermeasure for radio interference from legitimate radios located within a perimeter designed to block external emissions,
- The effective range of RF signals may be much longer than stated operating ranges, thereby allowing many attacks to occur using customized directed antennas and other technologies (see Section 2.3.3.3 for additional information on relevant operating ranges),
- Physical access controls do not protect against attacks by insiders (i.e., those granted access to the area),
- HERF/HERO/HERP still exists with respect to radiation emitted within the physical perimeter, and
- Due to the range of some RFID technologies, preventing physical access to the over-the-air communications may not be possible. In this case, an organization may try technical controls discussed in Section 5.3 to help mitigate eavesdropping or traffic analysis risks.

5.2.2 Appropriate Placement of Tags and Interrogators

Control: RFID system equipment can be placed to minimize unnecessary electromagnetic radiation. Tags and interrogators can be kept away from:

- Fuel, ordnance, and other materials that could *cause harm* if exposed to electromagnetic radiation,
- Humans and sensitive products (e.g., blood, medicine) that *might be harmed by* sustained exposure to RF subsystem radiation,
- Metal and reflective objects that can modify and amplify signals in unintended and potentially harmful ways, and
- Legitimate radios with which the RF subsystem communication will cause interference.

Applicability: All environments in which the organization deploying RFID systems determines the location of the RF equipment (which excludes many consumer and supply chain applications).

Benefits: Appropriate placement of interrogators and tags helps mitigate HERF/HERO/HERP, reduce interference with legitimate radios, and reduce the risk of eavesdropping and unauthorized RF subsystem transactions.

Weaknesses: This control has several potential weaknesses, including:

- Tag location cannot always be controlled, such as when tags are used to track mobile items (e.g., hospital cart) or items in transit (e.g., pallet on a truck).
- The complexity of the effects of RF energy on ordnance, fuel, and personnel make it difficult to predict the extent to which radio placement would mitigate HERF/HERO/HERP.
- Radio interference may persist even if the tags or interrogators are placed in a new location that is still sufficiently close to other radios.[48]

[48] In this situation, a panel or wall of grounded wire fencing between the two RF sources is a possible alternative means to reduce interference.

5.2.3 Secure Disposal of Tags

Control: Secure disposal involves physically or electronically destroying tags, as opposed to just discarding them, when they are no longer needed to perform their intended function. Physical destruction involves manual tearing or shredding using a paper shredder. Electronic destruction can be accomplished by using a tag's kill feature or using a strong electromagnetic field to render a tag's circuitry permanently inoperable.

Applicability: RFID applications in which the continued operating presence of a tag after it has performed its intended function poses a business intelligence or privacy risk (e.g., an adversary can subsequently use the presence of the tag to track items or people).

Benefits: Permanently disabling tags eliminates the possibility that they could be used later for tracking or targeting. For example, destroying or deactivating a tag can protect customers' privacy after the sale of a tagged item, which prevents adversaries from exploiting the mere presence of RFID tags to later identify individuals or otherwise adversely impact personal privacy. Destruction also prevents access to sensitive data stored on tags. When a tag supports an electronic disabling mechanism, it usually is the preferred way to destroy a tag before it is disposed because it can be accomplished without touching each tag, thereby reducing the cost of the effort.

Weaknesses: Even if minimal, the effort it takes to destroy a tag might increase the tag's lifecycle cost, which is a concern if very low costs are required to justify an RFID-enabled business process. Another potential weakness is that destruction of a tag precludes the ability to use it for future value-added applications. For example, a tag disabled or destroyed at checkout could not be used for recalls and additional product support at a later date.

Methods that disable a tag's radio functions could still allow an adversary with physical access to a tag to obtain data from it. For example, the EPC *kill* command disables the ability to execute subsequent commands but may not destroy the tag's memory.

5.2.4 Operator and Administrator Training

Control: Operator and administrator training provides personnel with the skills and knowledge necessary to comply with RFID usage and IT security policies, as well as agreements with external organizations. In most RFID implementations, personnel will perform various roles, which might require different training materials for each role. For example, an administrator of middleware might need different information than the operator of a mobile interrogator. Appropriate security training addresses at least three points:

- What constitutes unauthorized use,
- How to detect that unauthorized use might be occurring, and
- To whom to report violations.

If HERF/HERO/HERP risks are present, appropriate security training covers mitigation techniques, such as safe handling distances.

If tags are destroyed or recycled, training should cover how to perform these functions. For example, operators might be trained how to clear tag memory before reuse.

Applicability: All RFID implementations.

Benefits: Operator training helps ensure that the system is used and maintained properly. Training also helps operators identify security violations and take appropriate actions to prevent their reoccurrence.

Weaknesses: Training alone cannot ensure proper operation of the system or compliance with policy.

5.2.5 Separation of Duties

Control: RFID system duties are distributed among various personnel roles to minimize the damage resulting from an inadvertent or malicious activity of a single person. The general principle of the control is that malicious collusion between two or more authorized users is much less likely than one person engaging alone in inappropriate behavior.

One example of separation of duties is having different personnel (1) attach tags to objects and (2) read the tags. If an individual performed both functions, the individual could intentionally put the wrong tag on an object to circumvent the objectives of the business process. For example, a store clerk could affix tags intended for low-priced items on high-priced items, and then later work the checkout scanner while the clerk's accomplice purchased the items. The system would not know that the tags had been switched, but if another person performed the checkout, he or she might be suspicious of the checkout total, which could uncover the plot.

Applicability: RFID applications in which an insider might have a motive to perform unauthorized RFID transactions. This scenario is most likely to occur when tags support commercial transactions, especially those related to high-value objects.

Benefits: Separation of duties helps to reduce fraud and malicious damage, because any user attempting to engage in such activities would be forced to collude with at least one other user. Separation of duties also reduces errors, because a second operator will often catch mistakes made or missed by the first.

Weaknesses: Multiple employees still could collude to commit fraud or violate the RFID usage policy. Also, organizations with a limited staff may not be able to perform complete separation of duties.

5.2.6 Non-revealing Identifier Formats

Control: RFID tags are assigned identifiers using identifier formats that do not reveal any information about tagged items or the organization operating the RFID system. Non-revealing identifier format options include serially assigning identifiers and randomly assigning identifiers.[49]

Applicability: Any RFID tag that has a programmable identifier. Even tags that are designed to support standard tag formats can still be assigned non-standard identifiers in the field. However, some tags have factory-initialized identifiers that cannot be modified after manufacture.

Benefits: Adversaries that can read tags or eavesdrop on RF communication should not be able to gain any additional information from that identifier alone. In contrast, if an adversary reads an identifier that is

[49] A related control is rotating identifiers. Auto-routing tags store a list of identifiers and cycle through the list when queried. To support multiple identifiers, databases in the enterprise subsystem must associate each identifier in the list to the particular item. The benefit of rotating identifiers is that organization can make it more difficult to identity and track particular items as well as hide the type of item. Random and serialized identifiers, on the other hand, may not reveal information about the type of item, but since these identifiers are fixed, once they revealed that particular item can be tracked. One weakness to rotating identifiers is that a rogue reader can easily obtain the complete list of identifiers through repeated queries. Therefore, this control is more appropriate when the primary threat is eavesdropping. While research is being conducted on the concept of rotating identifiers, it is not specified in any RFID standard and proprietary designs are not widely commercially available.

encoded with a standardized format, such as the EPC format, that adversary may be able to discern the manufacturer or issuer of the item, as well as the type of item. For example, all cans of a soft drink from a certain manufacturer will have the same domain manager and object class bits if their identifiers are encoded in an EPC identifier format.

Weaknesses: This control has several weaknesses:

- The use of non-revealing identifier precludes an organization from realizing benefits that come from standard identifier formats that reveal organization and item type information. For example, standard identifier formats are particularly advantageous when designing and maintaining distributed databases in inter-enterprise systems. Lookup and query functions are much easier in such databases when the identifiers provide information on where item data is located.
- If identifiers are assigned randomly, then the identifiers must be managed so that two tags are not assigned the same identifier. Issuers of tags within the RFID system must have access to a list of all previously issued identifiers or accept the risk of collisions (i.e., two items being associated with the same identifier).
- If there is logic in how the identifiers are assigned, an adversary may uncover the method that is used, which would defeat the control. For example, an adversary knows that an identifier was assigned to a certain item and that all items of that type were assigned sequentially, then the adversary may be able to deduce the approximate range of identifiers that correspond to items of that type. Similarly, when identifiers are serialized, the adversary may be able to deduce the approximate time of the assignment based on the identifier.

5.3 Technical Controls

There are a number of technical controls currently available for RFID systems, and many others are under development in industrial and university research labs. This section divides the currently available technical controls for the RF subsystem into two groups:

- Controls to protect tag data, and
- Controls to protect RF communication.

These controls are discussed in depth in Sections 5.3.1 and 5.3.2, respectively. Many controls also exist for the enterprise and inter-enterprise subsystems, but these typically apply to IT systems in general rather to RFID systems in particular. Readers are encouraged to read other NIST IT system and network security guidance documents. Appendix D contains a list of relevant NIST security guidance publications.

5.3.1 Tag Data Protection

Technical controls currently available for protecting tag data include:

- Tag memory access controls, which can restrict use of tag commands and protect data stored in a tag's memory,
- The kill feature, which can prevent subsequent unauthorized use of a tag,
- Encrypting the data on tags,
- Fallback identification technology, which can complement tags in case of RFID system failure,

- Authentication, and
- Tamper protection.

These controls are described in more detail in Sections 5.3.1.1 through 5.3.1.4.

5.3.1.1 Tag Access Controls

Control: Tag command and memory access controls include access passwords and lock features. Different RFID standards implement these access controls differently or may not support these features at all.

Access passwords provide access control for a tag's commands and memory. The interrogator sends the access password before or in conjunction with a command to perform a protected function. For example, EPC Class-1 Generation-1 tags and EPC Class-1 Generation-2 tags both require a password to lock memory and to execute the *kill* command. Proprietary tag designs also use passwords to prevent reading of tag data and to temporarily disable or wake up a tag.

In particular, access passwords support some tags' lock feature, which provides read and/or write protection to memory. In some RFID technologies, the lock feature is permanent and in others it is reversible. For example, the EPC Class-1 Generation-2 *lock* command can be applied to five areas of memory and the memory becomes either read- and write-protected or only write-protected if it is locked.[50] The EPC Class-1 Generation-2 UHF standard also has a *permalock* feature. If engaged, permalock will make the lock status (locked or unlocked) permanent for all or part of a tag's memory. Finally, the ISO 18000-3 standard describes a *lock pointer*, which is a memory address. All areas of memory with a lower address than the lock pointer are write-protected.

Applicability: All applications that use a tag technology that supports passwords or memory locking. Organizations implementing RFID technology should consult tag manufacturers' technical specifications to determine if and how these features are supported.

All EPC tags and ISO 18000-3 tags support passwords. Both the EPC Class-1 Generation-1 and EPC Class-1 Generation-2 tags also support a *lock* command. Only EPC Class-1 Generation-2 tags support the permalock feature.

Benefits: Tag passwords can prevent unauthorized access to tag data, as well as unauthorized execution of commands such as *lock* or *kill*. There are also proprietary tag designs that use passwords for read access control. A write-protect *lock* command will prevent the contents of a tag's memory from being altered. A read-protect *lock* command will prevent unauthorized users from reading or accessing the data on tags.

Weaknesses: This control has a few significant weaknesses:

- The password length on many tags is too short to provide meaningful protection (e.g., EPC Class-1 Generation-1 tags support an 8-bit password, which provides only 256 possibilities for an adversary to guess). If a locked tag has no password protection or the password is weak (i.e., short or easily guessed), then unauthorized users can lock and unlock the tag at will.

[50] The five areas of memory are registers for the Kill password, access password, EPC memory, TID memory, and User memory. When locked, the Kill password and Access password become both read and write protected. If they are locked, the EPC memory, TID memory, and User memory are only write protected.

- The challenges of tag password management preclude the use of password guidance commonly associated with IT systems (e.g., a unique complex password that changes every 90 days). If tags are transferred from one organization's control to another, the organizations must determine how to transfer the passwords. If the same password is always used for all tags, then any party that learns the password could gain unauthorized access to all tags' data or functions. If different passwords are assigned to each tag, but the passwords are easy to guess (i.e., based upon a simple algorithm, such as the last digits of each tag's serial number), then the passwords will not be effective. Hard-to-guess passwords provide better protection, but may prove difficult to use without a mechanism for safely and securely sharing the passwords, which could result in the organization being unable to read or modify its own tags.

- Locking a tag's memory does not prevent data loss from electromagnetic interference or physical tag destruction.

- Cryptographic keys and access passwords on passive tags are subject to power analysis attacks, but specific conditions are necessary for a successful attack.[51]

5.3.1.2 Kill Feature

Control: A kill feature can permanently disable a tag's functionality using a remote command. The most common implementation of the kill feature is the EPC *kill* command. The *kill* command is password-protected using a password different from the access password.

Applicability: Applications that still experience business intelligence and privacy threats after a tag has performed its intended function (e.g., a tag may be used to track an individual's whereabouts after purchasing a tagged garment). EPC tags are the only standard-based tags that support a kill feature.

Benefits: Using the kill feature prevents a tag from being reused improperly. The kill feature was designed and implemented in EPC tags primarily to protect consumer privacy. It also protects improper access to tag data used in business processes. For example, discarded tags that have not been disabled may be read by adversaries to gain access to data, such as which products an organization or individual is purchasing or using.

Weaknesses: This control has several potential weaknesses, including:

- The existence of a kill feature represents a significant business process threat to an RFID system. If an adversary improperly disables tags that should remain in operation, the supported application will not function properly because it will not be able to perform transactions on the disabled tags. Furthermore, once killed, a tag cannot be used for any further application involving the asset (e.g., recalls, product returns).

- If a tag has no password protection for the *kill* command or the password is weak (e.g., short, poorly chosen), unauthorized parties can kill the tag at will.

[51] The power analysis attack (also called a side channel attack) is based on the fact some tags use different levels of power depending on how close the password provided is to the actual password. For instance, if the first bit in a password is incorrect, the tag uses less energy than it would if the eighth bit is incorrect, given how the algorithm is hard-coded into the tag's circuitry. These power differences are detected in the backscatter to the interrogator, but it requires that the adversary be reasonably close to the tag to get effective measurements. If such measurements are possible, an adversary can determine the password much more quickly than by using a brute force method. Lab experiments proved that someone could crack the 8-bit password protection found on EPC Class-1 Generation-1 tags in one minute. Source: Shamir, A., "Power Analysis of RFID Tags," presented at RSA Conference 2006, San Jose, CA, 2006. http://www.wisdom.weizmann.ac.il/~yossio/rfid/

- Data stored on the tag is still present in the tag's memory after it is killed (although it can no longer be accessed wirelessly).
- Although the *kill* command was added to tags for consumer privacy, consumers cannot easily detect whether a tag has been deactivated.[52] Moreover, consumers typically cannot kill tags on their own because this action requires an interrogator and knowledge of the *kill* password.

5.3.1.3 Data Encryption

Control: Data stored on a tag is encrypted, possibly by the tag, but more commonly in the enterprise subsystem

Applicability: All applications that store additional data beyond an identifier on the tag that needs to be kept confidential on the tag. Proprietary designs support encryption, but EPC and ISO 18000 standards do not.

Benefits: Data encryption protects sensitive tag data from being read by individuals with unauthorized access to the tags.

Weaknesses: This control has several potential weaknesses, including:

- Data encryption requires a key management system, which can be complex to manage and operate.
- Cryptographic functions may introduce an unacceptable delay in RFID systems that require very fast read or write transactions.
- Cryptographic functions require additional power to complete, which could impact applications that use passive tags.
- Tags that support onboard encryption currently are more costly than those that do not. One reason for the increased cost is that onboard encryption requires additional logic gates to perform the necessary computations. For instance, most low-cost passive tags do not have enough logic gates to perform complex encryption algorithms.

5.3.1.4 Fallback Identification Technology

Control: A fallback identification technology provides an alternative means to identify, authenticate, or verify an object when the RFID system is unavailable or an individual tag is inoperable. Options include text labels and AIDC technology such as bar codes.[53] The fallback may consist of just an identifier, or it may also include additional data about the tagged object.

Applicability: All RFID applications.

Benefits: Duplicating stored data on a label provides a fallback in case of malicious or accidental tag damage, interrogator malfunction, or enterprise subsystem network outage. The redundant data can also be used to verify that tag data has not been altered improperly.

Weaknesses: This control has several potential weaknesses, including:

---

[52] This may open a door for future consumer products to test for the presence of passive RFID tags and probe their characteristics. It is hypothesized that cellular phones may be able to provide this service for EPC passive tags since cellular phones already operate in the 860 to 960 MHz band.

[53] If the RFID application's objective is to provide security or authentication, then a fallback technology such as holograms or other optical security features may be used.

- Damage to the tag could render both the stored data and the printed data unusable. Similarly, many enterprise subsystem outages that would affect the RFID solution would also affect its fallback alternative.
- The data stored on the label is visible, so it may be easier for unauthorized parties to gain access to it than it would be to read the data from the tag.
- The text label or bar code might not provide the same data capacity as RFID memory, although two-dimensional bar codes can encode at least as many bits as standards-based tag identifiers.
- Text labels and AIDC technologies are static, so they do not provide a complete fallback solution for applications in which tag data changes over time. However, some identification information is still likely to be better than none in most applications.

5.3.1.5 Authentication Mechanisms

Control: Some RFID tags support on-board authentication mechanisms to provide either mutual or one-way authentication mechanisms. Mutual or bi-directional authentication allows a tag to verify a legitimate reader and allows a reader to verify a legitimate tag. This type of authentication, while providing a high level of assurance, is complex to implement on passive RFID tags and is not widely used. In contrast, one-way authentication is typically used to mechanisms require either the reader to authenticate to the tag, or the tag to authenticate to the reader. Each of these mechanisms addresses a different type of risk, so care must be given to select the right control to address the risks of each system being designed. Tag-to-reader authentication is used when it is important to verify the authenticity of the tag (and the object it is attached to)—which helps reduce the risk from tag cloning and replay. Reader-to-tag authentication is important in applications when only legitimate readers should have access to the data on the tag. In both cases, there are numerous technologies available to provide advanced authentication, and most of these are non-standard and proprietary implementations. In many cases, these mechanisms are still in development within the research and academic communities and are not yet commercially availability. Some examples of these advanced authentication technologies include: hash locking, hash-chaining, variable or randomized tag identifiers, digital signatures, cryptographic challenge response, and lightweight authentication protocols.

Applicability: These mechanisms are available on certain several types of contactless smart card tags. Since these types of devices are commonly used for applications that require higher levels of assurance—such as point-of-sale, banking, and access control—reader and card authentication is very important. In supply chain applications, where EPC tags are common, authentication is not often available or required. Most supply chain applications for RFID are engineered for low-cost, high-volume tag production. These mechanisms are not found in currently available EPC tags.

Benefits: Mutual authentication provides a high level of assurance in tag-to-reader transactions. One-way reader-to-tag authentication prevents an adversary from using a rogue interrogator to read tags. Mutual authentication prevents an adversary from using either rogue interrogators or rogue tags. Tag-to-reader authentication prevents an adversary from cloning, replaying, or spoofing legitimate tag identifiers.

Weaknesses: Like other security features, authentication mechanisms are limited by the strength of the method of implementation.

5.3.1.6 Tamper Resistance

Control: Certain RFID tags have tamper resistant or tamper-evident features that help prevent an adversary from removing the tags from the object to which they are attached. One simple type of tamper

resistance is the use of a frangible antenna; if a tag of this type is removed, the electric connection with the antenna is severed, rendering the tag virtually inoperable. Other, more complex types of RFID systems are used to monitor the integrity of objects associated with the tags – to ensure that the objects have not been compromised, altered, or subjected to extreme conditions. For example, this type of technology is being evaluated by the U.S. government for securing cargo containers while they are in transit between ports.

Applicability: Tamper resistance and tamper-evident features are currently only available on specialty RFID tags that are designed for tamper resistance to support specific buyer requirements.

Benefits: This control helps to prevent adversaries from breaking the association between a tag and its corresponding object. The more complex tamper-resistant / tamper-evident tags provide health and status monitoring of the attached objects to ensure that they have not been opened, manipulated, damaged, or subjected to extreme temperature, humidity, or shock.

Weaknesses: Sophisticated adversaries may be able to defeat the tamper resistance mechanisms. This is dependent upon the implementation of the tamper resistance feature. For example, a sophisticated adversary may be able to repair a frangible antenna. In addition, tamper-resistance / tamper-evidence technologies do not prevent the theft or destruction of the tag or its associated items.

5.3.2 RF Interface Protection

Several types of technical controls focus on the RF interface to tags, including:

- The selection of an operating radio frequency can be used to avoid interference from other sources or achieve certain operating characteristics such as the ability to propagate through metals, liquids, and other materials that are opaque to many frequencies.
- Interrogator and active tag transmission characteristics can be tuned to reduce the likelihood of eavesdropping and help mitigate interference and the hazards from electromagnetic radiation.
- Shielding can be installed to limit eavesdropping and rogue scanning.
- Cover-coding can be used to obscure the content of messages from interrogators to tags.
- The RF interface for active tags can be shut off to prevent unauthorized access.

These controls are discussed further in Sections 5.3.2.1 through 5.3.2.6.

5.3.2.1 Radio Frequency Selection

Control: RFID technology can communicate over various radio frequencies, including those in the LF, HF, UHF, and microwave bands. An RFID system can use a specific operating frequency to mitigate risk it might realize on other frequencies. Ideally, an RF site survey will be performed before an RFID system is installed to determine what frequencies are already in use. After the RFID system is installed, site surveys can be conducted to determine if the RF characteristics of the site have changed (e.g., new sources of interference).

Applicability: All implementations whose radio frequency is not determined by other application requirements. Organizations that implement a closed RFID system have more freedom to select an operating frequency because they do not have to interoperate with other organizations. However, if tags are based on a particular air interface standard, the range of potential frequencies will be limited to those supported by the standard.

Benefits: Radio frequency selection permits the avoidance of RF interference with other radio systems that could disrupt the RFID system or other technologies. A particular frequency might be desirable because of radio interference on other frequency bands. Some frequencies also have desirable propagation characteristics, such as the ability to penetrate certain materials.

Weaknesses: This control has the following potential weaknesses:

- It may be difficult to identify sources of interference. For example, bug zappers have been found to create interference in passive RFID trials.[54] Interference can be caused by poorly grounded motors, noisy relays, old fluorescent light ballasts, and other devices that generate unintended RF noise in nearby environments. Each RFID technology deployment should be tested in its intended environment prior to production use to identify these sources if interference.
- New sources of interference can be later introduced at the site.
- When implementing an open RFID system, all organizations involved in the system will have to agree on a tag type that supports all the frequencies that the organizations collectively intend to use.

Additional Information: Table 5-1 lists common sources of RF interference.

Table 5-1. Common Sources of RF Interference

Frequency Range	RFID Applications	Possible Interference Sources in U.S.
Less than 500 kHz	Animal tagging, access control, track and traceability, inventory control, car immobilizer, and EAS systems used in retail stores	Maritime radio and radio navigation
1.95 MHz - 8.2 MHz	EAS systems	Amateur radio, maritime mobile, land mobile, and aeronautical mobile
13 MHz - 13.56 MHz	EAS systems, access control, and smart cards	Older cordless phones, radio astronomy, and radio devices that use frequencies in the ISM bands.
430 - 460 MHz	Supply chain and in-transit visibility	Amateur radio, radio location, and land mobile radio
902 - 916 MHz	Railcar, toll road applications, and supply chain	Amateur radio, radio location, cordless phones (900 MHz), and other ISM applications
2.35 - 2.45 GHz	Real-time location systems (RTLS), and supply chain	Cordless phones (2.45 GHz), Wi-Fi, Bluetooth, radio location, satellite, and ISM applications
5.4 - 6.8 GHz	Intelligent transportation systems[55]	Cordless phones (5.8 GHz), aeronautical navigation, radio navigation, and amateur radio

5.3.2.2 Transmission Power Adjustment

Control: Many interrogators can be adjusted to reduce the level of transmitted RF energy. Additionally, the duty cycle of an interrogator can be adjusted.

Applicability: All interrogators with adjustable transmission power.

[54] Sullivan, Laurie, "IBM Shares Lessons Learned From Wal-Mart RFID Deployment", InformationWeek, Oct 15, 2004.

[55] For additional information on intelligent transportation systems, see http://www.itsa.org/its_technologies/c9/What_is_ITS/ITS_Technologies.html.

Benefits: Reducing transmitted power can:

- reduce the likelihood that an adversary can intercept communication,
- limit radio interference with other legitimate radios, and
- lessen HERF, HERO, and HERP.

Weaknesses: The drawback of reducing transmission power or the duty cycle is performance degradation, especially with respect to back channel communication from a passive tag. For instance, interrogators might fail to detect the presence of valid tags. Also, changes in the physical environment or the introduction of new radio equipment can impact the power levels required for consistently successful transactions. Consequently, the benefits of power adjustments based on a site survey can be negated by changes to the environment.

5.3.2.3 Electromagnetic Shielding

Control: RF shielding encloses an area with a conducting material that limits the propagation of RF signals outside of the shielded area. Shielding can vary in size and form depending on the application.

For example, some travel documents that are equipped with RFID chips have a metallic anti-skimming material. If the passport is closed, this material helps to prevent adversaries from reading the RFID chip inside. Shipping containers are sometimes shielded to prevent the reading of tags during transit. Shielding is also placed in walls, partitions, or stalls to prevent RF emissions from leaving a confined area. When interrogators are placed in tunnels on industrial production conveyor belts, the tunnels may be shielded to reduce radio interference.

Figure 5-1 shows how shielded partitions can separate collocated interrogators to prevent interference. The interrogators near forklift A can operate without inadvertently reading tags on boxes on forklift B due to the shielding in the partition that separates the portals. Shielding may be necessary when middleware is unable to correctly filter duplicate read events from the two portals.

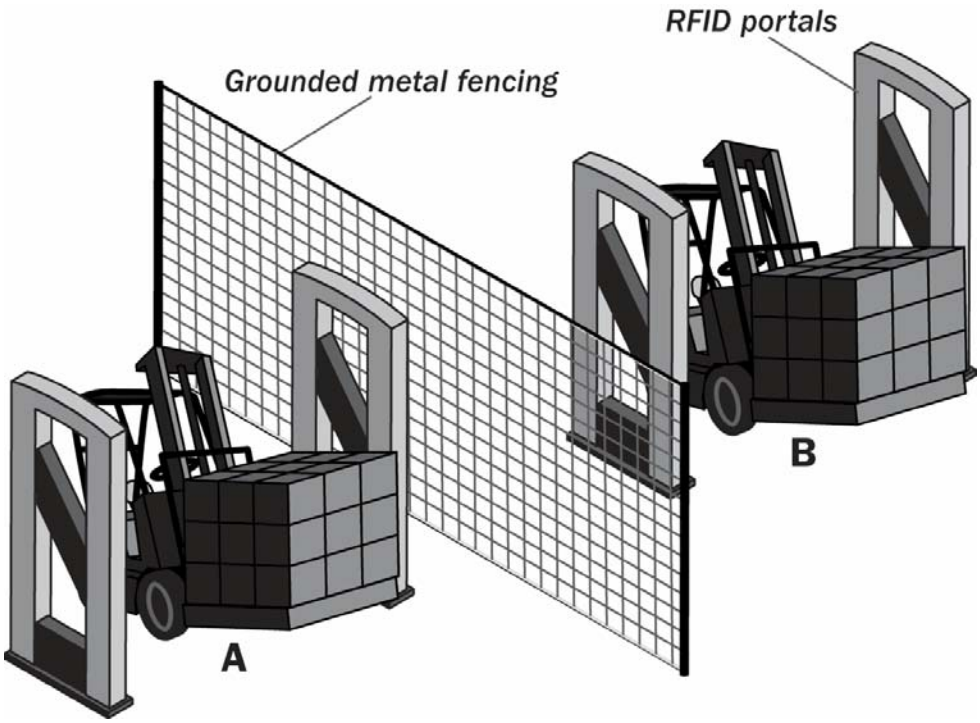

Figure 5-1. Grounded Metal Fencing as Shielding

Applicability: Shielding is applicable for contexts in which eavesdropping, RF radiation, or interference is a concern, and the placement of shielding would not stop valid transactions.

Benefits: Shielding can limit the ability of eavesdroppers or unauthorized interrogators to collect data from an RFID system. Shielding can also reduce the propagation of RF radiation, which is helpful in situations where there are HERF/HERO/HERP hazards.

Weaknesses: This control has a few potential weaknesses, as follows:

- Shielding can prevent or hinder legitimate transactions. For example, shielded containers require objects to be physically removed from the container. This prevents an implementing organization from realizing one of the key benefits of RFID technology, which is to read tags remotely without optical line of sight and additional handling.
- It may still be possible for an adversary to place a radio inside the shielded area. The radio could be used for malicious purposes, such as eavesdropping on RFID transactions or causing interference.

5.3.2.4 Cover-Coding

Control: Cover-coding is a method for hiding information on the forward channel from eavesdroppers. The cover-coding method relies on the fact that the interrogator forward channel signal strength is much greater than RFID back channel signal strength, making the back channel signal less likely to be intercepted. In the EPC Class-1 Generation-2 standard, cover-coding is used to obscure passwords and information written to a tag using the *write* command.

The EPC Class-1 Generation-2 cover-coding protocol works as follows:

1. The interrogator sends a message to the tag requesting a key.
2. The tag generates a random 16-bit number (i.e., the key) and returns it to the interrogator.
3. The interrogator produces ciphertext (i.e., a message unintelligible to an eavesdropper) by applying an exclusive-or (XOR) operation[56] to the key and the plain text.
4. The interrogator sends the ciphertext to the tag.
5. The tag applies the XOR operation using the ciphertext and the key it generated to recover the plain text.[57]

Applicability: EPC Class-1 Generation-2 is a standards-based solution that supports cover-coding. Proprietary technologies support similar features. Cover-coding is designed for RF subsystems in which the forward channel carries stronger signals than the back channel, which essentially limits the control to passive tags.

Benefits: Cover-coding significantly increases the difficulty of eavesdropping because it requires an adversary to intercept signals on the back channel, as well as the forward channel. Intelligible reception of back channel signals from a passive tag requires proximity of less than four meters in most applications. In many applications, an adversary's reception equipment would be conspicuous if it were located within this range. In contrast, interrogator signals can be detected at distances on the order of kilometers under ideal conditions.

Cover-coding prevents passwords from being transmitted over-the-air in clear text, which helps prevent the execution of unauthorized commands that could disable a tag or modify the tag's data. Consequently, cover-coding mitigates business process, business intelligence, and privacy risks.

Weaknesses: This control has a few potential weaknesses, as follows:

- If an adversary can intercept a key distributed on the back channel, it could decrypt any ciphertext message generated with that key.
- The effectiveness of cover-coding depends on the performance of the tag's random number generator. If the random number is predictable due to a flaw in the tag's design, then an adversary can learn the key and decrypt subsequent communication.

5.3.2.5 Temporary Deactivation of Active Tags

Control: The RF interface on some proprietary active tags can be turned off temporarily. Tag manufacturers have different methods of turning their tags on and off. For example, some tags are designed so that the tag is on or off depending upon which end is inserted into a mounting clip. Other tags have replaceable batteries that can be removed to deactivate them. Some tags can be programmatically turned off through their over-the-air interfaces.

For instance, tags may be turned on inside a designated area where the RF subsystem operates. When the tags leave that area, they would be turned off. For example, in a supply chain application, tags may be

---

[56] The XOR operation is a binary operation denoted with the symbol "⊕" that works as follows: $1 \oplus 1 = 0$; $1 \oplus 0 = 1$; $0 \oplus 1 = 1$; $0 \oplus 0 = 0$. When the XOR operation is applied to two multi-bit strings, the XOR operation is applied to the first bit of the each string to produce the first bit of the result, the second bit of each string to produce the second bit of the result, and so on. To work properly, the inputs to the XOR operation must be of equivalent length, and the output is also of the same length.

[57] The XOR operation is symmetric. For instance, given key K, plaintext P, and ciphertext C, if $P \oplus K = C$, then $C \oplus K = P$.

turned off to prevent unauthorized transactions during shipment. When the tags arrive at their destination, they would be powered on again and managed. Conversely, active tags used for in-transit visibility may be turned on for their trip and turned off when they reach their destination.

Applicability: Applications that use active tags where the tag manufacturer has provided a capability to turn tags on and off. Some tags have internal tamper-resistant features that ensure that the tags are never turned off.

Benefits: This control can mitigate certain RF security vulnerabilities, such as targeting and unauthorized tag reads. This control is most useful when communication between interrogators and a tag is infrequent and predictable. In addition to addressing security concerns, turning off tags when they are not in use extends tag battery life.

Weaknesses: This control has a few potential weaknesses, as follows:

- If operators or system software fail to reactivate the tag when it is needed, then the missing transactions resulting from the tag's RF silence could adversely impact the supported business process.
- If turning a tag on or off requires human intervention, then this control would result in additional labor expense, which could be significant for systems that process large numbers of tags. The potential increased labor effort required to operate the system could negatively affect the business case for RFID relative to other AIDC technologies.
- Even if the activation and deactivation process is automated, it introduces a delay that might not be acceptable for many time-sensitive applications.

5.4 Summary

Organizations should use a combination of management, operational, and technical controls to mitigate the business risks of implementing RFID systems. Table 5-2 maps the presented controls to the categories of risks that they mitigate. Because each RFID implementation is highly customized and each organization's requirements are different, the security controls discussed in this section are not all applicable or effective for all RFID applications. Organizations need to assess the risks their RFID implementations face and choose the appropriate controls, taking into account factors such as regulatory requirements, the magnitude of threats, and cost and performance implications of the controls. For example, a remote warehouse may have little need to protect against eavesdropping, but it may require redundant processes in case of system failure. Traditional security controls are often preferable to RFID-specific controls. For example, if an RF tag contains only a serial number that is meaningless without access to a corporate database, then normal IT security controls safeguarding the database are probably more practical than trying to encrypt each tag's serial number.

Table 5-2. RFID Controls Summary

		Risk Mitigated by Control				
					4.4 Externality Risk	
	Control	4.1 Business Process Risk	4.2 Business Intelligence Risk	4.3 Privacy Risk	4.4.1 Hazards of Electro-magnetic Radiation	4.4.2 Computer Network Attacks
Management	5.1.1 RFID Usage Policy	X	X	X	X	X
	5.1.2 IT Security Policies	X	X		X	
	5.1.3 Agreements with External Organizations	X	X	X	X	
	5.1.4 Minimizing Data Stored on Tags	X	X	X		
Operational	5.2.1 Physical Access Control	X	X		X	X
	5.2.2 Appropriate Placement of Tags and Interrogators	X	X			X
	5.2.3 Secure Disposal of Tags	X	X	X		
	5.2.4 Operator and Administrator Training	X	X		X	X
	5.2.5 Separation of Duties	X				
	5.2.6 Non-revealing Identifier Formats		X	X		
Technical	5.3.1.1 Tag Access Controls	X	X	X	X	
	5.3.1.2 Kill Feature			X		
	5.3.1.3 Data Encryption	X	X	X		
	5.3.1.4 Fallback Identification Technology	X				
	5.3.1.5 Authentication	X	X	X	X	
	5.3.1.6 Tamper Resistance	X	X			
	5.3.2.1 Radio Frequency Selection	X				X
	5.3.2.2 Transmission Power Adjustment		X			X
	5.3.2.3 Electromagnetic Shielding		X	X		X
	5.3.2.4 Cover-Coding					
	5.3.2.5 Temporary Deactivation of Active Tags		X	X		

Table 5-3 reviews how common RFID standards support selected controls discussed in this section.

Table 5-3. Control Applicability to Selected RFID Standards for Asset Management Applications

Control		ISO 18000-3	EPC Class-0	EPC Class-1 Generation-1 UHF	EPC Class-1 Generation-2
Guide Reference	**Supporting Features**				
Minimizing Data Stored on Tags (5.1.4)	User-defined memory	Up to 8 Kbytes	Not supported	Not supported	Supports user memory without limited maximum memory size
Destruction of Retired Tags (5.2.3)	Kill feature	Not supported	Supported	Supported	Supported
Tag Access Controls (5.3.1.1)	Kill password	Not supported	Supports a 24-bit password	Supports a 8-bit password	Supports a 32-bit password
	Access password	Mode 2 supports a 48-bit memory access password. If required, the password both read and write protects all areas of memory.	Not supported	Supports write protection for the identifier	Supports a 32-bit password that can selectively provide read and write protection for passwords and write protection for all other memory
	Lock pointer	Mode 2 supports a lock pointer that write protects all memory addresses less than the pointer.	Not supported	Not supported	Not supported
Kill Feature (5.3.1.2)	Kill feature	Not supported	Supported	Supported	Supported
Data Encryption (5.3.1.3)	Integrated encryption	Not supported	Not supported	Not supported	Supports one-time pad stream cipher to write data to tags and to transmit passwords
	User-defined memory	Supported	Not supported	Not supported	Supported

6. RFID Privacy Considerations

All organizations that implement and maintain systems that use, collect, store, or disclose personally identifiable information (PII) (also known as "information in identifiable form") should understand the Federal privacy laws, regulations and policy that can impact the integration and operation of RFID systems. This section provides a list of privacy considerations and controls that can help organizations understand the business risks of implementing systems with RFID technology. Since RFID implementations are typically highly customized, the privacy controls listed are not always applicable or may not be effective for all RFID systems. Organizations should also frequently assess the current landscape of Federal privacy laws and regulations as these laws and regulations change often. Finally, organizations should work with legal counsel when developing its privacy approach to ensure that the approach is consistent with applicable laws and regulations.

While many organizations must implement privacy controls to comply with legal mandates, other organizations may implement privacy controls for other reasons other than legal compliance, such as to maintain or enhance their reputation or as part of an overall program of social responsibility. Therefore, even if an organization is not legally bound to comply with certain privacy restrictions, it may still review related laws and regulations to develop and enforce its own privacy policy.

6.1 Privacy Principles

Organizations should consider a comprehensive approach for managing information at the system and program levels that is based on laws, regulations, and a thorough understanding of privacy-related risks. This can best be accomplished by establishing an integrated approach that addresses PII as part of an overall RFID strategy. The development of a set of baseline privacy requirements will assist organizations in quickly and efficiently addressing privacy-related requirements. A set of widely applicable privacy principles would provide a common set of privacy requirements relevant for public and private sector organizations, including organizations that operate outside of the United States.

Below are commonly identified privacy principles provided by the Organization for Economic Cooperation and Development (OECD) that are reflected in its Fair Information Practice Principles. The material offered in this section is offered neither as an endorsement of OECD's overall privacy posture nor an endorsement of the privacy posture of any one or group of its members. Table 6-1 lists OECD definitions of its privacy principles.

Table 6-1. OECD Privacy Principles[58]

#	Privacy Principle	Definition
1	Collection Limitation	There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
2	Data Quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, and be kept up-to-date.
3	Purpose Specification	The purposes for which personal data are collected should be specified not later than at the time of the data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

[58] The principles and definitions in this table are those found in "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD, 1980

#	Privacy Principle	Definition
4	Use Limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the specified purpose.
5	Security Safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6	Openness	There should be a general policy of openness about developments, practices, and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, the main purposes of their use, as well as the identity and usual residence of the data controller.
7	Individual Participation	An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him (1) within a reasonable period of time, at a charge, if any, that is not excessive, in a reasonable manner, and in a form that is readily intelligible to him; (2) (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and (d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed, or amended.
8	Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

6.2 Federal Privacy Requirements for Federal Agencies

Different Federal privacy statutes exist for different types of organizations. Some laws are relevant to financial organizations, while others are relevant to health care organizations. This section focuses on Federal privacy rules and guidance that pertain to Federal agencies. Commercial organizations that handle, process, or share data with Federal agencies may also be covered by these rules and guidance. Other organizations may not be covered, but may still have an interest in learning how they might incorporate Federal privacy practices to improve their own privacy programs.

The major Federal privacy requirements impacting Federal agencies include:

- Privacy Act of 1974,
- Section 208 of the E-Government Act of 2002,
- Section 522 of the Consolidated Appropriations Act of 2005,
- Administrative simplification requirements of the 1996 Health Insurance Portability and Accountability Act (HIPAA),
- FISMA, and
- OMB memoranda on the implementation of privacy requirements.

A more comprehensive listing of privacy-related laws and regulations can be found in Appendix XX, “Privacy-related Laws, Regulations and Policy”.

For over 30 years, the cornerstone of federal information privacy law has been the Privacy Act of 1974 (“the Privacy Act”), (5 U.S.C. 552a), which was written before the widespread adoption of IT as the primary means of managing data. The Privacy Act regulates the collection, use, maintenance, and dissemination of personal information about U.S. citizens or aliens lawfully admitted for permanent

residence. The Privacy Act applies only to records about individuals maintained by agencies in the executive branch of the government. It also only covers information filed within a "system of records." A system of records is a group of files that:

- Contain an individual's name, Social Security Number (SSN), or some other unique personal identifier (such as employee number) AND one other element of personal information about the individual (such as date of birth); and
- Are retrieved by an individual's name, SSN, or personal identifier.

Section 208 of the E-Government Act of 2002 ("Section 208") prescribes the establishment of a privacy framework for agencies to manage compliance with privacy mandates passed since 1974. Section 208 privacy mandates include:

- Designating a point of contact for privacy roles and responsibilities,
- Ensuring employees, business partners and contractors are informed and educated of their responsibility to protect PII,
- Performing privacy impact assessments (PIAs) when developing, acquiring, or purchasing a new IT system, and also when one or more of the nine changes or "PIA triggers" occur,
- Ensuring website privacy policies and notices are updated and adhere to Federal requirements,
- Complying with website tracking technology requirements and developing and implementing a machine-readable privacy policy plan, and
- Evaluating IT system and business model privacy risks for program activities and their information systems.

The privacy requirements in Section 522 of the Consolidate Appropriations Act ("Section 522") are prescribed for the Departments of Treasury and Transportation, as well as Independent Agencies. However, all agencies should consider compliance with Section 522 as a privacy best practice and program goal, especially if the organization is a business associate to one or more of the above agencies. Section 522 mandates, which are far reaching and more comprehensive than previous laws, are designed to extend the privacy requirements in Sect. 208 of the E-Government Act of 2002. In summary, Section 522 requires the following:

- Assuring that the use of technologies sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in an identifiable form,
- Assuring that technologies used to collect, use, store, and disclose information in identifiable form allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use and distribution of information in the operation of the program,
- Assuring that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as defined in the Privacy Act of 1974,
- Evaluating legislative and regulatory proposals involving collection, use, and disclosure of personal information by the Federal Government,
- Conducting a privacy impact assessment of proposed department rules on the privacy of information in an identifiable form, including the type of personally identifiable information collected and the number of people affected,

- Preparing a report to Congress on an annual basis on activities of the department that affect privacy, including complaints of privacy violations, implementation of section 552a H. R. 4818—461 of title 5, 11 United States Code, internal controls, and other relevant matters,
- Ensuring that the Department protects information in an identifiable form and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction,
- Training and educating employees on privacy and data protection policies to promote awareness of and compliance with established privacy and data protection policies,
- Establishing privacy and data protection procedures and policies,
- Ensuring compliance with the departments' established privacy and data protection policies,
- Recording with each agency's Inspector General a written report of the agency's use of information in identifiable form, along with its privacy and data protection policies, and
- Each agency shall have performed an independent, third party review of the use of information in identifiable form as the privacy and data protection procedures of the agency.

The final privacy and security rules of the HIPAA administrative simplification requirements represent the first nationwide effort to protect an individual's personal health information from unwarranted access and disclosure. Both sets of regulations make up two critical sides of the patient information confidentiality. Privacy regulations focus on the application of effective policies, procedures and business service agreements to control the access and use of patient information. The security regulations address the organization's infrastructure requirements to assure secure and private communication, as well as the maintenance of confidential patient information.

FISMA was implemented in order to ensure a more consistent and efficient means to evaluate the security of information systems and to improve existing systems within the federal government that are lacking in security measures. Subsequent OMB guidance, Fiscal Year (FY) 2006 Instructions for Preparing the FISMA and Privacy Management Report, prescribes that in order to carry out these goals that information and information systems must be categorized and have the appropriate number of security controls and privacy considerations given to each. In addition, there must be a mechanism in place to monitor the security controls, as well as to determine the deficiencies of the system. The monitoring mechanism is a quarterly FISMA report.

OMB has issued several memoranda in the past few years providing policy guidance and instructions for the implementation of privacy requirements. Among these privacy-related memoranda are:

- OMB M-03-22: Guidance for Implementing Section 208 of the E-Government Act of 2002,
- OMB M-05-08: Designation of Senior Agency Officials for Privacy,
- OMB M-06-15: Safeguarding Personally Identifiable Information,
- OMB M-06-16: Protection of Sensitive Agency Information,
- OMB M-06-19: Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, and
- OMB M-06-20: FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management.

6.3 Applicable Privacy Controls

The following integrated compliance and risk management methodology provides an approach for capturing privacy requirements and potential controls for an organization's RFID system. Benefits of embedding privacy controls into RFID systems include:

- Ensuring performance objectives, business processes, service-components, technologies, and data each appropriately maps to privacy requirements;
- Describing privacy in the context of IT controls aids in standardizing and consolidating privacy capabilities as appropriate; and
- Understanding which privacy controls, when implemented correctly, will demonstrate compliance, risk management and industry best practices across a number of Federal privacy laws, regulations and policy.

The Federal Chief Information Officers (CIO) Council ("CIO Council") developed the following privacy taxonomy as a reference model for describing 17 privacy control families. The control families may be used for Federal information systems, programs, and enterprises for the collection, storage, sharing and transmission of PII. A common taxonomy can prove particularly useful for organizations that implement RFID technology. These following privacy control families may be useful in identifying controls that may be useful to achieve privacy compliance requirements, industry best practices and privacy risk management mechanisms[59]:

- Policies and Procedures – Creating policies and procedures governing the appropriate use of personal information and implementing privacy controls,
- Privacy as Part of the Development Life Cycle – Implementing privacy reviews and controls throughout the system development life cycle (SDLC),
- Assigned Roles, Responsibilities, and Accountability – Identifying general and specific roles and responsibilities for managing and using personal information and ensuring accountability for meeting these responsibilities,
- Monitoring and Measuring – Monitoring the implementation of privacy controls and measuring their efficacy,
- Education: Awareness and Role-based Training Programs – Ensuring managers and users of personal information are made aware of the privacy risks associated with their activities and of applicable laws, policies, and procedures related to privacy,
- Public Disclosure – Publicly disclosing privacy policies and procedures for a program or system,
- Notice – Providing notice of the information practices to the individual before collecting personal information,
- Consent – Gaining consent from the individual to use their personal information,
- Minimum Necessary – Collecting the minimum amount of personal information necessary to accomplish the business purpose,

[59] These privacy controls will vary depending on the other aspects of an organization's RFID system, technologies and business processes. For example, the line of business and functions for federal transportation initiatives and delivery of healthcare medical devices to retired veterans will likely have a very different set of privacy controls. However, both would likely need to have privacy controls within the notice and consent family.

- Acceptable Use – Ensuring that personal information is used only in the manner provided on the notice, to which the individual consented, and in accordance with the publicly disclosed practices,
- Accuracy of Data – Ensuring that personal information is accurate, particularly if harm or denial of benefits may result,
- Individual Rights – Providing individuals an opportunity to access and correct their personal information and to seek redress for privacy violations,
- Authorization – Ensuring that the individual authorizes all new and secondary uses of personal information not previously identified on the original collection notice,
- Chain of Trust – Establishing and monitoring third-party agreements for the handling of personal information,
- Risk Management – Assessing and managing risks to operations, assets, and individuals resulting from the collection, sharing, storing, transmitting, and use of personal information,
- Reporting and Response – Providing senior managers and oversight officials the results of the monitoring and measuring of privacy controls and responding to privacy violations, and
- Security Measures – Implementing the appropriate safeguards to assure confidentiality, integrity and availability of personal information.

6.4 Embedding Privacy Controls

Organizations can use a three-phased approach to identify and apply privacy controls to achieve an integrated privacy compliance and risk management strategy:

- Step 1: Identification – Identify privacy requirements and capabilities. For a system or program, all applicable laws and regulations, as well program-specific policies and procedures should be analyzed and categorized according to the privacy control families. Similarly, technologies and services that either directly support of have privacy support components should be captured.
- Step 2: Analysis – Analyze unmet requirements and review current and planned capabilities to identify opportunities to consolidate, re-use, or invest through a trade-off analysis. Map requirements to capabilities and identify unmet requirements that need to be addressed. Seek opportunities to leverage other non-privacy capabilities to meet a privacy function and analyze capabilities to identify those that may be re-used to meet a requirement, such as capabilities that are redundant or could be consolidated. Perform a trade-off analysis to identify the cost/benefits of each solution.
- Step 3: Selection – Evaluate proposed solutions, and select the solution that best meets the organization's requirements. This stage ensures that privacy considerations are appropriately incorporated into the solution and that the selected solution does not introduce new risks.

While numerous scenarios exist that could comprise the privacy or confidentiality of individuals' PII, Figure 6-1 offers an illustrative sample of questions and high level guidance on how organizations implementing RFID systems may evaluate the privacy impact of RFID applications.

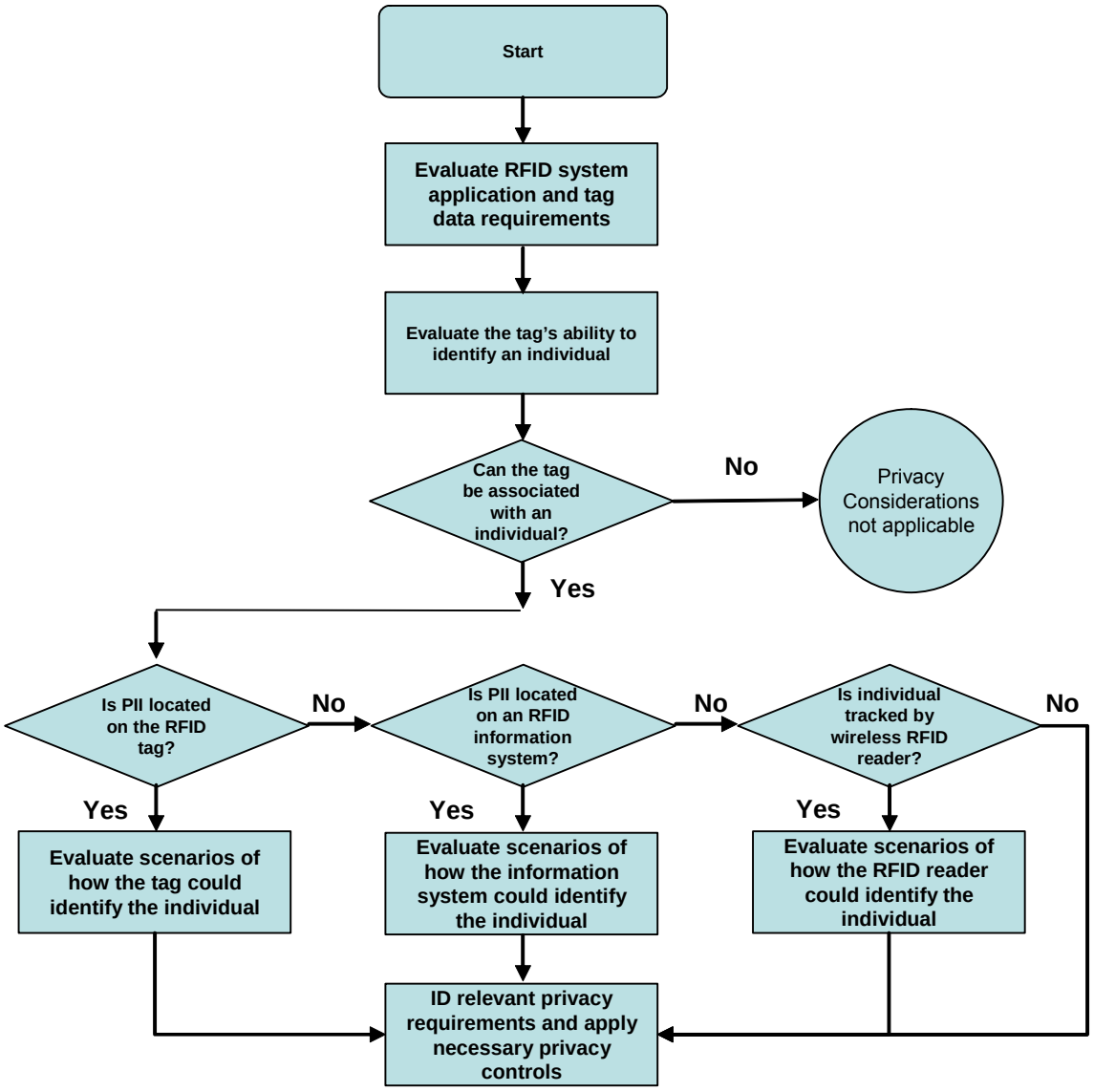

Figure 6-1. Sample Process for Evaluating RFID Privacy Impact

Organizations that identify, understand, and implement the requirements of privacy laws and regulations are better positioned to ensure the privacy of PII associated with RFID systems. Additionally, organizations should solicit the collaboration and expertise of their designated senior agency official for privacy, as well as other privacy compliance-related officials for the appropriate identification and integration of privacy controls into RFID systems and technologies.

Organizational privacy stakeholders may include, but are not limited to IT officials who may reside in the Office of the Chief Information Officer (OCIO), Office of the Special Counsel or Office of the Privacy Advocate, and the Privacy Act, Disclosure and/or Freedom of Information Act (FOIA) Officers. This collaboration of RFID project managers and privacy officials will help ensure greater understanding of privacy initiatives currently in place, provide for greater efficiencies in the use and sharing of agency resources, and lowers the risk and/or costs of RFID projects. Additionally, collaboration can better enable

RFID project managers to ensure privacy controls are considered early in the SDLC and avoid costly retrofitting of solutions.

6.5 Summary

A critical success factor for organizations implementing and managing RFID systems is the identification and understanding of applicable privacy laws, regulations and policy that may impact the initiation, design, implementation and operation of RFID. The ability to translate these privacy requirements into IT business needs enables organizations to engineer privacy controls into the RFID SDLC and project management life cycles.

7. Recommended Practices

As explained in Sections 2 through 5, there are numerous ways to implement and configure RFID systems to support a wide variety of applications. RFID solutions typically must be highly customized to support the business processes they automate; no one-size-fits-all approach will work across implementations. Nevertheless, organizations can benefit from following some general principles when using RFID technology. This section describes a set of recommended security practices that can help organizations manage RFID risks to an acceptable level.

To be most effective, RFID security controls should be incorporated throughout the entire life cycle—from policy development to operations. This section references a five-phase life cycle to help organizations determine the most appropriate actions to take at each point in the development of the RFID system. The life cycle is based on a model introduced in NIST Special Publication (SP) 800-64, *Security Considerations in the Information System Development Life Cycle.* [60] Organizations may follow a project management methodology or life cycle model that does not directly map to the phases presented here, but the types of tasks and their sequencing are probably similar. The phases of the life cycle are as follows:

- **Phase 1: Initiation**. This phase covers the tasks that an organization should perform before it starts to design its RFID solution. These tasks include conducting a risk assessment and developing policy and requirements with which the RFID solution must comply.
- **Phase 2: Acquisition/Development.** For the purposes of this guide, the Acquisition/Development phase is split into two sub-phases:
  - **Phase 2a: Planning and Design**. In this phase, RFID network architects specify, the standards with which the RFID system must comply, the network infrastructure that will support the system, and the technical characteristics of the RFID solution, including the types of tag and interrogators that will be deployed,. This phase should also include site surveys of the facilities and relevant IT infrastructure.
  - **Phase 2b: Procurement**. In this phase, the organization specifies the RFID components that must be purchased, the feature sets and protocols they must support, and any standards on which they must be based.
- **Phase 3: Implementation**. In this phase, procured equipment is configured to meet operational and security requirements, RFID data is integrated with legacy enterprise systems, and staff are trained in the proper use and maintenance of the system.
- **Phase 4: Operations/Maintenance**. This phase includes security-related tasks that an organization should perform on an ongoing basis once the RFID system is operational, including conducting periodic security assessments, applying security-related software patches, and reviewing RFID event logs.
- **Phase 5**: **Disposition.** This phase encompasses tasks that occur when a system or its components have been retired, perhaps as a result of a significant upgrade. These tasks include preserving information to meet legal requirements and disabling or destroying tags and other components when they are taken out of service.

The practices presented in this section are provided in tables corresponding to the life cycle phases. Each practice is accompanied by a brief explanation of the rationale for its inclusion and is rated as "recommended" or "should consider". Organizations are strongly encouraged to adopt the

[60] This document is available at http://csrc.nist.gov/publications/nistpubs/.

"recommended" practices. Failure to implement them significantly increases the risk of an RFID security failure. Organizations should also examine each of the "should consider" practices to determine their applicability to the target environment. A "should consider" practice should be rejected only if it is infeasible or if the reduction in risk from its implementation does not justify its cost.

Organizations should develop their RFID security controls based not only on the practices in the tables, but also using other guidance on security controls. FIPS Publication (PUB) 199 establishes three security categories—low, moderate, and high—based on the potential impact of a security breach involving a particular system.[61] NIST SP 800-53 provides minimum management, operational, and technical security controls for information systems based on the FIPS PUB 199 impact categories.[62] The information in NIST SP 800-53 should be helpful to organizations in identifying controls that are needed to protect networks and systems, which should be used in addition to the specific practices for RFID systems listed in this document.

The RFID policies that an organization develops should be consistent with existing IT and operations policies. However, in some cases, the organization may need to modify the existing policies to accommodate the introduction of an RFID system.

Some large organizations may divide RFID-related duties among various teams. For example, one group may be responsible for the RF subsystem, while another might focus on the enterprise subsystem. To assist with this division of labor, the tables in this section identify the impacted subsystem or components (e.g., tag or interrogator) for each of the listed practices.

The tables can also serve as checklists. In particular, the status column on the right is blank so that RFID support staff or auditors can use it to measure progress toward implementation of the practices.

[61] FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*, is available at http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf.

[62] NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*, is available at http://csrc.nist.gov/publications/nistpubs/.

Table 7-1. RFID Security Checklist: Initiation Phase

Initiation Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
1	Perform a risk assessment to understand RFID threats, the likelihood that those threats will be realized, and the potential impact of realized threats on the value of the organization's assets.[63]	All risks should be considered, including the risk of RFID systems to other enterprise information systems and the risk that the existence of RFID will enable adversaries to collect information about an organization's activities that could adversely impact its ability to perform its mission. The risk assessment should also explicitly state whether or not fuel or ordnance is anticipated to be located within the operating range of the RFID system. Additionally, it should cover any potential impacts to human health resulting from use of the RFID technology. For supply chain applications, the risk assessment should consider threats that occur when the RFID tags are located outside the organization's control, such as when tagged items are in transit. The risk assessment is an important input to the development of the RFID usage policy because it identifies which RFID activities pose an acceptable risk to the organization's information resources and which do not. In particular, it can help determine which type of RFID technology may be appropriate for the desired application (e.g., active versus passive tags).	ALL	Recommended	

[63] For more information on performing risk assessments, read NIST SP 800-30, *Risk Management Guide for Information Technology Systems*. All NIST SPs are available for download from http://csrc.nist.gov/publications/nistpubs/.

Initiation Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
2	Establish an RFID usage policy that specifies what assets should be tagged, who is authorized to use RFID technology, and for what business purposes this authorization applies.	AN RFID usage policy is the foundation on which subsequent security controls are based. The policy should cover all components of the RFID system, including tags, interrogators, and support systems (e.g., middleware and analytic systems). The policy should distinguish between the levels of access provided to those that use the system, those that administer it, and those that need access to its data, including external business partners. For instance, logistics administrators may be granted the ability to modify an interrogator's configuration (duty cycle, power output, network settings, RF frequency settings, Transmission Control Protocol (TCP) ports, etc.) while operations personnel may only be able to scan tags. External parties should almost never get access to an organization's interrogators, but they might need read access to certain database elements. The policy should also address the collection and handling of sensor data that might be transmitted over the RFID system. Finally, if blocker tags or other RF countermeasures are anticipated, the policy should cover how they will be implemented and managed. In particular, they should not be permitted inside a warehouse because they will disrupt automation and logistics processes.	ALL	Recommended	
3	Establish an RFID privacy policy.	Federal government agencies are required to create a Privacy Impact Assessment (PIA) if the RFID system will store or manage personal information. While privacy policy is not within the scope of this guidance, the technical security controls that result from the policy are within the scope of the guidance. For example, implementation of the privacy policy might require the use of the *kill* command or an alternative means to disable tags. Requirements related to data sharing limitations may need to be supported by certain authentication and access control methods. The privacy policy should be in place first for the RFID system architects to determine the appropriate security controls.	ALL	Recommended	

Initiation Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
4	Establish HERF/HERO/HERP policies.	If the risk assessment identifies risks related to human health, fuel, ordnance, or other sensitive materials (e.g., pharmaceuticals) that are not fully mitigated by the RFID usage policy, then the organization should require additional controls to prevent the associated hazard from being realized. A separate policy is needed for each hazard type (HERF/HERO/HERP/other sensitive materials) because each one has distinct issues. Organizations facing these hazards should also consult safety and regulatory experts in this area to ensure their approaches are valid and meet requirements.	RF Subsystem	Recommended	
5	Enhance a network security policy to account for the presence of RFID systems.	The introduction of RFID technology represents a new threat to the security of the enterprise network that should be mitigated by policy and associated technical, operational, and management controls. Elements of the network security policy that might be impacted include perimeter security (i.e., firewalls and extranets) and wireless connections (i.e., between interrogators and the enterprise network). Typically a firewall separates interrogators from the enterprise network that hosts RFID database and application servers. In addition, if interrogators are connected to the enterprise infrastructure via a wireless link, then the policy should require mutual authentication between the interrogator and its network access point. It should also provide for data confidentiality and integrity services for wireless traffic, if needed.	ALL	Recommended	
6	Establish an RFID security training program for operators of the RFID system.	Many RFID risks are best mitigated when the personnel operating the system are aware of the risks and the associated countermeasures. The training program should cover the RFID usage policy and teach administrators and operators how to identify and report violations of the policy. This may be coupled with general training on the operation of the RFID system.[64]	ALL	Should Consider	
7	Use professionals with training or experience in RFID technology and information security to assist with design and implementation of the RFID system.	Wireless security is a complex field. Even small flaws in implementation can have significant ramifications for the resulting security of the RFID solution. Well-trained RFID professionals can help mitigate this risk.	ALL	Recommended	

[64] NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, contains detailed guidance on designing, developing, implementing, and monitoring an IT security awareness and training program.

Table 7-2. RFID Security Checklist: Planning and Design Phase

Planning and Design Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
8	Identify the RFID standards with which the RFID system will comply.	The selected RFID standards in effect determine the types of tags that will be deployed and the operating frequencies on which RF subsystem communication will occur. Standards and their associated tag types characterize the risks that should be managed. For example, active tags have risks that passive ones do not, such as greater vulnerability to data integrity and confidentiality attacks due to their longer range. The standards also specify the available technical security mechanisms. For instance, some tags support passwords while others do not. An organization may also choose a standard to support a particular operating frequency to avoid unwanted RF interference, improve performance, and reduce technical problems. The choice of operating frequency is often closely associated with the relevant application area (e.g., healthcare, supply chain, security access control, and animal tracking).	RF Subsystem	Recommended	
9	Conduct a site survey to determine the proper location of interrogators and other devices given a desired coverage area.	The estimated usable range of interrogators and tags should not extend beyond the physical boundaries of the facility whenever possible. The survey should note the location of metal or reflective objects that have the potential to adversely impact the operation of the RFID system. The site survey should also identify potential radio interference between the RFID system and other RF sources at the site or in neighboring facilities.	RF Subsystem	Recommended	
10	Determine approach to RF emissions control.	The approach should be based on the risk assessment and site survey. In many cases, physical security may offer the best mechanism to protect against unauthorized use of RFID technology, including attacks involving interrogator spoofing and jamming, modification of tag data, and eavesdropping. When this is not possible, countermeasures such as shielding and adjusting the power level of the interrogator may be employed. The selected approach might involve the location of interrogators and tagged assets, the placement of blocker devices, the power levels at which RF components operate, and the potential need for additional perimeter security (e.g., fences around warehouses).	RF Subsystem	Recommended	

Planning and Design Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
11	Design a dedicated VLAN[65] to support the RFID system.	Using dedicated VLANs to support RFID connections to the enterprise network segregates RFID traffic from other network communications. Dedicated VLANs also facilitate the use of network access control lists (ACL) that identify the protocols and services that are allowed to traverse routers that connect RFID local area networks to other network segments.	Enterprise Subsystem and Interrogators	Should Consider	
12	Identify an approach to securing network management traffic, using dedicated networks and encryption when feasible.	If network management traffic is left unprotected, adversaries might be able to breach the RFID system, enabling a number of subsequent attacks, including those that could disable the system or compromise confidential data. The approach to securing network management traffic depends largely on the technical architecture. If network management occurs over web interfaces, then Secure Sockets Layer (SSL) or Transport Layer Security (TLS) should be employed. In some cases, devices such as interrogators will be managed using SNMP. In these cases, SNMP version 3 is the preferred approach, and community strings should be changed from defaults to complex character strings (i.e., mix of upper and lower case, both alphabetic and numeric characters).	Enterprise Subsystem and Interrogators	Recommended	
13	Design a network firewall between the RF subsystem and the enterprise network.[66]	A firewall can enforce a security policy on the information flow between the RF subsystem and any attached network, allowing only authorized protocols and services to traverse this boundary, such as those needed for interrogators to communicate with middleware servers and for management consoles to monitor and configure interrogators. This configuration limits the ability of an adversary that compromises RFID equipment to exploit vulnerabilities on non-RFID systems that also reside on the network. Appropriate firewall placement depends on the network architecture. For example, if middleware is integrated into the switches to which the interrogators connect, the firewall may be included in the switch or may reside between the middleware and the enterprise network. On the other hand, if middleware servers are located inside an enterprise network (e.g., at a remote data center), then the firewall may reside between the interrogators and the middleware.	Enterprise Subsystem	Should Consider	

[65] A VLAN is a logical group of hosts that communicate as if they were on the same physical Local Area Network (LAN), even though they might be on different ones. VLANs are created through the configuration of one or more switches across an enterprise.

[66] More information on network firewalls is available from NIST SP 800-41, *Guidelines on Firewalls and Firewall Policy.*

Planning and Design Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
14	Develop RFID audit processes and procedures that identify the types of security relevant events that should be captured, and determine how audit records will be securely stored for subsequent analysis.	Audit records are necessary for forensic analysis of security incidents and also support real-time intrusion detection capabilities in many cases. Ideally, audit data should be forwarded to a dedicated audit server that can preserve the integrity of event logs even when other RFID system components have been compromised. To facilitate implementation and compliance, existing audit processes and procedures for other enterprise information systems should be leveraged whenever appropriate. Events to be captured should include, at a minimum, unsuccessful authentication attempts.	Enterprise Subsystem and Interrogators	Recommended	
15	Determine a password generation scheme for tags that support password-protected features.	The security of password protection mechanisms is only as strong as the passwords.	Tags	Recommended	

Table 7-3. RFID Security Checklist: Procurement Phase

Procurement Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
16	Procure products that use FIPS-validated cryptographic modules.[67]	Federal agencies are required to use FIPS-validated cryptographic modules. Cryptographic modules that are not FIPS-validated cannot be assured of providing the level of cryptographic protection intended. Identify all expected uses of cryptography, including those that will be used to secure data traffic in the enterprise subsystem. Significant resource constraints on tags preclude the use of cryptography for many applications, but if an organization decides that the additional expense of cryptography is required to protect sensitive information, then the corresponding cryptographic modules must be FIPS-validated.	ALL	Recommended	

[67] For a listing of FIPS-validated cryptographic modules, visit http://csrc.nist.gov/cryptval/.

Procurement Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
17	Procure products that are functionally capable of supporting the organization's security policy.	If a product that does not support the security policy is deployed, non-compliance is guaranteed. For example, if the RFID usage policy requires data confidentiality between the interrogator and the enterprise subsystem, then the interrogators need to support appropriate cryptographic services on their enterprise interface. In general, tags do not have cryptographic data functionality, but data encrypted elsewhere can be stored on a tag if it has sufficient capacity, which typically is the case for active tags only.	ALL	Recommended	
18	Procure interrogators, middleware, and analytic systems that log security relevant events and forward them to a remote audit server in real time.	Audit technology helps ensure that the organization can detect unauthorized behavior and take actions to prevent or limit the extent of a security breach. If software components do not support audit event forwarding, then the organization should ensure that the supporting operating systems do so. At a minimum, the events should contain the tag ID, interrogator ID, and the interrogation timestamp for security relevant events.	Interrogators and Enterprise Subsystem	Recommended	
19	Procure interrogators and server platforms that support the selected approach to securing network management traffic.	The network management architecture only can be implemented if the selected products support it. Potential protocols include SNMP version 3 or the encapsulation of management traffic within SSL/TLS or Internet Protocol Security (IPsec) tunnels.	Interrogators and Enterprise Subsystem	Recommended	
20	Procure interrogators and server platforms that support Network Time Protocol (NTP).	NTP allows distributed devices to synchronize timestamps, which is critical to effective log analysis because it allows audit personnel to establish accurate event sequences across multiple devices. Many applications also need to obtain very accurate measurements of the time elapsed between transactions. Examples include industrial process applications and race time tracking applications.	Interrogators and Enterprise Subsystem	Recommended	
21	Procure an auditing tool to automate the review of RFID audit data.	Audit tools often are more effective than humans at distilling relevant information from multiple sources. In large enterprise RFID deployments, reviewing the amount of data generated could overwhelm technical support staff if they do not have appropriate tools to assist them with this task.	Enterprise Subsystem	Should Consider	
22	Procure interrogators that can be upgraded easily in software or firmware.	This capability enables the interrogators to receive security patches and enhancements released after product shipment.	Interrogators	Recommended	

Table 7-4. RFID Security Checklist: Implementation Phase

Implementation Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
23	Harden all platforms supporting RFID components (e.g., middleware, analytic systems and database servers).	Organizations should apply secure operating system and database configurations to all relevant hosts. See other NIST guidance for recommended configuration information.[68]	Enterprise Subsystem	Recommended	
24	Ensure that interrogators that support user authentication have strong, unique administrative passwords.	To protect against dictionary attacks, administrator passwords on interrogators should not be easy to guess.	Interrogators	Recommended	
25	Configure wireless interfaces on interrogators.	Interrogators may need to be tuned to avoid unnecessary electromagnetic emissions that could result in data compromise or other adverse effects (e.g., HERF, HERO, HERP). Tunable parameters include the transmission power level and the frequency at which the interrogator polls for tags. If the interrogator is mobile, it likely will have a second wireless interface to connect to the enterprise subsystem. In this case, the second interface should have a secure configuration.[69]	Interrogators	Recommended	
26	Assign unique passwords to tags.	When tags support passwords, organizations should not use a common password for multiple tags. Otherwise, a compromised password on one tag could have much wider consequences. Managing unique passwords requires the implementing organization to maintain a password database and support remote queries of the database, which might not be feasible in all environments.	Tags	Should Consider	

[68] The NIST Security Configuration Checklists Program for IT Products program collects checklists for securing various operating systems and applications. The checklist repository and information about the program are available at http://checklists.nist.gov/.

[69] See NIST SP 800-48, *Wireless Network Security: 802.11, Bluetooth and Handheld Devices* and NIST SP 800-97, SP 800-97, *Guide to IEEE 802.11i: Robust Security Networks* for information on how to secure common wireless protocols.

Implementation Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
27	Disable all insecure and unused management protocols on interrogators and enterprise subsystem components. Configure remaining management protocols for least privilege.	Disabling all insecure and nonessential management protocols eliminates potential methods that an adversary can use when attempting to compromise a host. Examples of insecure management protocols include SNMP version 1 and SNMP version 2. If SNMP version 3 is used, configure it for least privilege (i.e., read only) unless write access is required (e.g., to change configuration settings as part of an automated incident response procedure).	ALL	Recommended	
28	Activate logging and direct log entries to a remote audit server.	Logs enable security and support staff to identify potential security issues and respond accordingly. Using a remote central logging server facilitates reviews of logs across the enterprise and ensures the integrity of log data when RFID components are compromised.	Interrogators and Enterprise Subsystem	Should Consider	
29	Initiate a HERF/HERO/HERP compliance program to include operator training, posting of notices, and application of labels to sensitive materials.	If personnel are reminded of risks to their safety, they are more likely to engage in behavior that will prevent the realization of those risks. The compliance program should comply with Occupational Health and Safety Administration (OSHA) regulations regarding workplace safety.[70] Notices should appear in the same or comparable locations as other OSHA notices.	RF Subsystem	Recommended	

Table 7-5. RFID Security Checklist: Operations/Maintenance Phase

Operations/Maintenance Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
30	Test and deploy software patches and upgrades on a regular basis.[71]	Newly discovered security vulnerabilities of vendor products should be patched to prevent inadvertent and malicious exploits. Patches should also be tested before implementation to ensure that they work properly.	ALL	Recommended	

[70] For additional information, see rules on non-ionizing radiation. 29 CFR 1910.97. http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9745

[71] More information on patching is available from NIST SP 800-40 version 2.0, *Creating a Patch and Vulnerability Management Program*.

Operations/Maintenance Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
31	Review audit logs frequently.	Frequent reviews of audit logs allow security and support personnel to identify security issues and take corrective or preventative measures quickly. All components of the RFID solution should generate event logs. Automated logging tools can assist with log review and send real time alerts in response to critical events, such as repeated failed authentication attempts during a short time period. RFID middleware products often provide advanced audit capabilities, including "dashboards" that allow administrators to monitor the activities of interrogators in real time.[72]	ALL	Recommended	
32	Perform comprehensive RFID security assessments at regular and random intervals.	Security assessments, or audits, are an essential tool for checking the security posture of an RFID system and identifying corrective actions necessary to maintain acceptable levels of security. The assessments should include monitoring of the RF spectrum to determine potential sources of RF interference and to identify ongoing surveillance or attacks. The assessment should also verify configuration settings on all RFID components.	ALL	Recommended	
33	Designate an individual or group to track RFID product vulnerabilities and wireless security trends.	Assigning responsibility to an individual for tracking wireless security issues helps ensure continued secure implementation of the organization's RFID systems.	ALL	Should Consider	

[72] For additional information on audit log management, see NIST SP 800-92, *Guide to Computer Security Log Management* (DRAFT) at http://csrc.nist.gov/publications/drafts/DRAFT-SP800-92.pdf

Table 7-6. RFID Security Checklist: Disposition Phase

Disposition Phase					
#	Security Practice	Rationale / Discussion	Impacted Components	Recommended or Should Consider	Checklist Status
34	When disposing of tags, disable or destroy them.	The appropriate disposal or destruction mechanism depends on the type of tag, the level of assurance required, and the cost of the destruction. When tags contain memory, this memory should be rendered inaccessible. Options include the *kill* command and physical destruction. Many tags can be rendered inoperable by cutting them with a box knife, scissors, or other sharp object. The antenna on some tags can be separated from their transmitters by tearing them by hand. Even if a tag contains nothing but an identifier, destruction may be advisable if there is the potential for an adversary with knowledge of the tag encoding protocol to correlate the identifier with other information, such as tag ownership. This attack is particularly salient for EPC tags, because of the potential to look up information using ONS. In many cases, the tag identifier also reveals the serial number of the asset. On the other hand, many organizations may determine that that this risk is acceptable, especially if database records corresponding to a particular identifier are disabled when the tag is no longer needed.	ALL	Should Consider	
35	When disposing of an RFID component, ensure that its audit records are retained or destroyed as needed to meet legal or other requirements.	Information contained in the audit records may be needed even after an RFID component is discarded (e.g., for an investigation of a subsequently discovered security breach). Organizations should identify the legal requirements for data retention that apply to their operations.[73] When log events are forwarded to a central audit server, which is recommended, regular backup of the server facilitates the retention of records. When a log server does not exist, the disposal process may include capturing the existing log data and storing it on alternative media, such as CD-ROM or tape. On the other hand, retention of audit records may raise a privacy concern in some applications. For example, records may reveal sensitive personal information or associate a person with particular items or transactions in a manner that violates privacy laws or policy. In these cases, the requirement may be to destroy the records after a certain period of time or after they are no longer needed.	ALL	Recommended	

[73] An example of a requirements document is General Records Schedule (GRS) 24, *Information Technology Operations and Management Records.* GRS 24 is available from the National Archives and Records Administration at http://www.archives.gov/records_management/ardor/grs24.html.

This page has been left blank intentionally.

8. Case Studies

This section presents two case studies to illustrate how RFID security might be implemented in practice. Although the case studies are fictional, they are intended to resemble real-world activities, including how decision makers address common and expected RFID security problems and their solutions. The case studies do not cover *all* of the aspects of RFID system engineering or operations that an organization may encounter in its RFID implementation, but rather a representative sample of salient issues. The two case studies are as follows:

- Case Study #1: Personnel and asset tracking in a health care environment, and
- Case Study #2: Supply chain management of hazardous materials.

In each case study, the fictional organization followed the information system development life cycle introduced in NIST SP 800-64, *Security Considerations in the Information System Development Life Cycle,* and the practices discussed in Section 7.

8.1 Case Study #1: Personnel and Asset Tracking in a Health Care Environment

The Contagion Research Center (CRC) is a health care facility dedicated to the study of highly contagious diseases—those transmitted through casual human contact. The Center has 40 beds for patient care, a radiology unit with two rooms of sophisticated imaging equipment, and four laboratories with various diagnostic and research capabilities. The Center confronts the same management issues as many hospitals, including locating portable diagnostic equipment when needed and accounting for missing assets. Another important concern is the ability to quickly locate patients and staff as they move about the facility. Poor asset management results in higher costs, reduced efficiency, and lower quality of care.

The mission of the CRC also leads to specialized requirements. To prevent unnecessary outbreaks of disease and to understand how transmission occurs, CRC needs to track the interactions among its staff, patients, and visitors. These tracked interactions provide useful information to researchers about who came into contact with whom and at what time. Additionally, CRC must alert caregivers of disease-specific protocols when they are in close proximity to particular patients, including prohibiting staff contact in some cases. It must track blood, urine, and stool samples from patient to laboratory. Finally, CRC would like to track the history of in-house diagnostic equipment and trace how the equipment is used to support patients throughout each day. Currently, paper processes are used to achieve these objectives, but they are very labor-intensive and error-prone, sometimes with fatal consequences.

CRC's Chief Information Officer (CIO) believes that RFID technology offers a way for the CRC to both to improve its traditional asset management function, as well as meet its specialized requirements. Working with CRC executives and the CRC board of directors, she has commissioned a project to reengineer CRC business practices using RFID technology as a primary tool to improve organizational performance.

8.1.1 Phase 1: Initiation

The first step in the project was to conduct a risk assessment to help shape the final scope of the project and identify the most appropriate uses of the RFID technology, as well as potential controls to mitigate the accompanying risk. Some risks identified during the assessment were as follows:

- RFID systems could open a "backdoor" to the CRC computer network, which could result in the compromise of mission-critical systems and research archives.

- Anyone eavesdropping on RFID transactions could compromise the privacy of patient medical records.
- The CRC could be held liable for violations of the privacy provisions of Health Insurance Portability and Accountability Act (HIPAA).
- The radio frequencies used by the RFID system could interfere with wireless patient sensors and medical telemetry devices, which could impact quality of care and research results.
- RFID tags might be a potential vector for some highly contagious diseases.

The risk assessment also concluded that some RFID risks were minimal or nonexistent in the CRC environment. The worst case for expected patient and staff exposure to RF radiation was forecasted to be significantly below any level that might adversely affect their health. CRC already had a well-enforced policy that prohibits the storage of fuel or ordnance at the facility, and the use of potentially explosive material such as ether and oxygen tanks was tightly controlled. The likelihood that an adversary would attempt to use the CRC RFID system to gather intelligence or target personnel was deemed negligible.

As a result of the risk assessment, the CRC enhanced its network security policy to require that the RFID system be separated from other network systems using a firewall that permits only required data and management traffic to traverse the network boundary. The network security policy also was amended to require user authentication to all non-stationary RFID interrogators and encryption of wireless traffic between mobile interrogators and access points. Existing policy regarding secure server configurations and least privilege[74] data access would extend to the RFID systems without requiring any modifications. The CRC also decided that it would not institute a new requirement for wireless intrusion detection, but it would revisit this decision during the following fiscal year.

The CRC privacy policy was also revised to account for the introduction of RFID technology. The revision noted that any patient data collected by the RFID system would be subject to the CRC's internal procedures implementing HIPAA regulations. Although the staff debated whether RFID risks needed to be disclosed to patients given that reasonable safeguards were being applied, a final determination was made to update patient release forms to include a statement that inherent risks exist with wireless communications and that network security controls were implemented to help mitigate these risks.

Based on the project charter and the updated security and privacy policies, the CIO led an interdisciplinary team of medical practitioners and information technology professionals to develop the business and functional requirements for the RFID system. These requirements formed the basis for the phases of the project that followed.

8.1.2 Phase 2: Acquisition/Development

The acquisition and design phase of the project involved planning the RFID solution. One design decision was to select the tag type for each application. Many of the items to be tracked, including laboratory samples and disposable supplies, were numerous and would be scanned at very close ranges (within 10 centimeters). For these items, passive tags made the most sense, given their low cost. People, high-value assets, and mobile equipment such as carts, gurneys, and wheelchairs needed to be tracked as they moved around the facility. The readable range for these applications needed to be at least a few meters. The team considered active tags, but worried that they could cause interference problems when located in the radiology unit. Accordingly, they selected semi-active tags, which are less likely to emit

[74] The principle of least privilege in computer security refers to the concept of granting each user and each module of a system only the necessary resources to perform authorized actions.

radiation inadvertently and which have a considerably longer battery life than active tags, but which still have effective operating ranges within CRC's requirements.

The next step was to plan the location of the stationary interrogators and the frequencies at which they would operate. In preparation for this exercise, CRC had qualified individuals perform a site survey, which recommended locations for the interrogators and identified existing spectrum utilization within the facility. They found that patient sensors and medical telemetry devices were operating at low frequencies (125 kHz) and at ultra high frequency ranges (915 MHz). Frequencies throughout and above the radio spectrum were identified in the radiology unit. Based on this information, the design team determined that the passive RFID system would operate in the high frequency range (13.56 MHz), and the semi-active RFID system would operate at microwave frequencies (2.45 GHz).

While the risk of eavesdropping from locations outside the facility was considered to be very low, the design team still thought it would be of value to mitigate the risk to the greatest extent feasible. Therefore, they ensured that design drawings placed interrogators away from windows and exterior walls. Preferred locations were over doorways in rooms and on ceiling mounts in hallways. The devices would be prohibited in the radiology unit, but would be placed at entries to the unit. Previously installed shielding in the walls would prevent emissions from impacting the operation of the imaging equipment inside the unit.

The design team determined that stationary interrogators would be connected to the RFID middleware infrastructure using Ethernet, which is also used to network the desktop computers and servers in the building. To accomplish this, the plan called for the installation of additional network cabling and drops, and use of the existing Ethernet switches, which had considerable excess capacity. Having the RFID systems, desktops, and servers all cabled into the same switches created a risk that the RFID system could be used as a platform to launch an attack on the rest of the network. To mitigate this risk, the design called for a dedicated VLAN to host the RFID-related network hosts. Traffic could only pass from the RFID VLAN to other network segments if it traversed the network firewall required by policy in the Initiation Phase.

Once the architecture was completed, the CIO assigned two members of the design team to the job of procuring the system with her review and approval. They paid particular attention to the products' audit and management capabilities. Four vendors provided demonstrations of their products and submitted bids.

8.1.3 Phase 3: Implementation

The various components of the system arrived over a three-week period following the procurement effort. The implementation team followed the CRC secure configuration guidelines when building all the servers hosting RFID enterprise software and databases. The implementation team configured all the audit events and alerts on the RFID systems to be directed to a CRC audit server cluster that supports all of the CRC IT infrastructure. They also ran a vulnerability scan on all hosts after the installation to identify remaining weaknesses. Approximately a dozen minor issues were discovered and quickly resolved, mostly through the application of software patches. The last step in preparing the infrastructure was to configure the firewall traffic filters and VLAN architecture specified during the Acquisition/Development phase.

Applying tags to all the items within the scope of the project was a challenging and time-consuming task. When possible, tags were positioned on items in such a way as to minimize the probability of tampering, destruction, or removal. They were also placed where patients are unlikely to experience dermal or respiratory contact, therefore reducing the probability that a tag's surface could ever be a mechanism for

the spread of disease. Tags on patients were embedded in hospital admission wrist bracelets. Tags for staff and hospital personnel were embedded in their hospital identification cards, which are typically worn around the neck on a lanyard or on a retractable leash attached to the belt.

8.1.4 Phase 4: Operations/Maintenance

The operation of the new systems proceeded as expected. CRC experienced a reduction in asset lossings resulting from better tracking and some personnel mentioned that they system significantly reduced paperwork. The system also provided benefits to CRC research. In one case, patients in separate rooms under the supervision of different medical teams contracted a particular illness. These facts initially led the CRC epidemiologists to believe that an airborne pathogen caused the disease. Subsequent analysis of the RFID data showed that a medicine cart handled by several nurses' aides was the likely infection vector by transferring the disease from patient to patient through dermal contact.

The operations phase also included the management of the RFID system. Hospital IT personnel received pages when systems were malfunctioning and took corrective actions as necessary. Recently, audit records showing excessive numbers of malformed read transactions led to the detection of an unauthorized radio in the proximity of one of the interrogators.

8.1.5 Phase 5: Disposition

The new RFID system has not been in operation long enough to encounter significant disposition issues, but the CRC has instituted procedures for the disposal of RFID tags. The passive tags on disposable items are discarded along with the item. In the case of tags on blood, urine, and stool samples, the tags are disposed as hazardous medical waste. Semi-active tags on patients are disposed of as medical waste upon death or discharge. Data did not need to be removed from the tags prior to disposal because the tags only stored an identifier. Semi-active tags on physical assets are reassigned when the asset is retired. If a tag is malfunctioning, it is physically disabled to ensure inoperability and discarded with office waste.

8.1.6 Summary and Evaluation

The system involving read-only passive and semi-active tags is helping reduce costs and improve research. Security risks were identified early, and risks were managed to an acceptable level. Table 8-1 presents a summary of how each risk identified in the risk assessment was subsequently addressed.

Table 8-1. CRC Risk Management Strategy

Risk	Mitigation Approach
Exploitation of "backdoor" to IT network	• Stationary interrogators kept away from windows and exterior walls • VLAN isolates RFID network from other network segments • Network firewall restricts traffic to/from RFID network • Servers hosting RFID middleware, analytic systems, and databases are built with secure configurations • RFID audit events are sent to centralized audit server that is continuously monitored by operations personnel
Compromise of patient information confidentiality	• Stationary interrogators kept away from windows and exterior walls • Risk disclosed to patients and caregivers

Risk	Mitigation Approach
Radio interference with diagnostic sensors and equipment	• 13.56 MHz frequency selected to minimize interference with other devices
Spread of disease	• Tag placement minimizes chances of dermal or respiratory contact • Tags in contact with patient or lab samples are discarded as medical waste

8.2 Case Study #2: Supply Chain Management of Hazardous Materials

The Radionuclide Transportation Agency (RTA) oversees the movement of radioactive research materials between production facilities, national laboratories, military installations, and other relevant locations. The RTA oversight of the supply chain for these materials involves many of the same issues as in most any other supply chain. The agency wants to know who is in possession of what quantity of materials at any given time. It also wants to locate materials at a site quickly, without having to search through numerous containers to find them. Bar code technology does not provide that capability.

Some of RTA's requirements are more unique. For instance, much of the transported radionuclide material must be closely monitored because extreme temperatures or excessive vibration can make it useless for its intended applications. Consequently, RTA wants temperature and vibration sensors to continuously measure environmental conditions and record readings on the tag. Additionally, the handling of RTA-regulated materials is a homeland and national security issue. If the materials were to fall into unauthorized hands, they could endanger the public welfare.

8.2.1 Phase 1: Initiation

The project team began with a risk assessment, which identified a number of concerns, the most significant of which were as follows:

- An adversary could identify and target a vehicle containing RTA-regulated material.
- An adversary could eavesdrop on tag transactions to learn the characteristics of the material, which could help determine whether it is worth stealing.
- An adversary could damage or disable a tag, making it easier to steal material without detection.
- An adversary could alter sensor or manifest data stored on the tag in an effort to undermine the business processes for which the material is being used.
- An adversary could corrupt the tag naming service, which would make it easier to hide the misdirection or theft of tagged materials.
- The radiation from interrogators could accidentally cause combustion of collocated volatile materials when several of them are operating concurrently in close proximity.

To help address the risks, the RTA established a policy that required that tagged items only be identifiable during embarkation, debarkation, and storage, but not during transport. The policy further stated that tag-interrogator communication should be authenticated whenever technically feasible with commercial-off-the-shelf solutions. Finally, it required that all personnel involved in handling of the tagged materials be provided RFID security awareness training. The agency already had a HERF policy, but everyone agreed the introduction of the RFID system would require the agency to revisit the efficacy of these HERF-related controls.

8.2.2 Phase 2: Acquisition/Development

The acquisition/development phase focused on the planning and design of the RFID solution. The nature of the supply chain was such that tagged items would be located at numerous facilities, including future facilities not yet known at time the design was created. However, some general parameters were known. For instance, interrogators would need to read tags from distances up to 10 meters, and this capability is typically only found in active tags.

The design team spent a significant amount of time on how to mitigate risks associated with the RF link between the interrogators and the tags. It determined that the risk of eavesdropping and rogue RFID transactions could be within acceptable levels if adversaries were located at least 100 meters from the storage area.[75] The few facilities that could not maintain a perimeter of that distance would rely on bar code technology, which RTA understood would significantly increase labor costs at these sites relative to those using RFID because people would need to be hired to scan items and open containers to inventory their contents.

To address the requirement of preventing readings during transport, the design team specified mechanisms for shielding containers and vehicles. The shielding would prevent adversaries from determining that items inside a vehicle were tagged, thereby reducing the risk of targeting. In the case of shielded transport vehicles, tags could be read when they were removed from the vehicle at debarkation. Many vehicles were shielded prior to the RFID program to prevent harmful radiation from escaping the vehicle. When vehicles were not shielded, tarp-like shielding could be replaced around containers within the vehicle and then easily removed when they leave the vehicle. While some users would benefit from the convenience of reading tags from outside the vehicle, the risk this introduced outweighed any potential advantage it offered. Indeed, the primary objectives of the RFID system were to identify the facility at which a radionuclide sample was located and to quickly find items once stored, neither of which necessitated readings when the item was in transport.

The tags were also password-protected using a proprietary technology to prevent unauthorized parties from reading or writing to the tags. Because custody of the tags moved from one organization to another, the RTA decided to host a central password database that could be remotely accessed by the RFID middleware of each participating organization. To limit access to the central database to business partners, it was placed on a VPN called RTAnet to which each of the partner organizations connected. The VPN isolates the RFID activity from public networks, thereby making it difficult for an outside adversary to perform a successful attack.

The team also had to tackle the HERF risk. Although the probability was small that interrogators would cause combustion of volatile materials stored near radionuclide material, the devastating consequences of its realization still made it a significant concern. The primary mechanism was to use an HF system because it would be less likely to cause combustion than higher frequency UHF and microwave technology. New guidelines also required a separation of five meters between fuel and tagged items unless the volatile materials were shielded.

8.2.3 Phase 3: Implementation

The implementation phase was straightforward, given the extensive planning in the previous phase. The first task was to conduct a pilot test of the system to identify potential problems before they adversely impacted the full supply chain. The test exercise uncovered several interoperability issues with RTAnet

[75] The risk was determined by field tests to be acceptable because the 100 meter distance was shown to prevent eavesdropping of tag to interrogator communications.

devices. In particular, some of the interrogators did not work properly with the middleware solution because an undocumented feature conflicted with the settings RTA selected for its equipment. The vendor issued a patch to its software that solved the problem.

8.2.4 Phase 4: Operations/Maintenance

Once the system was fully operational, the RTA was able to obtain regulatory information more quickly than previously, which reduced the labor time required to support the program. Suppliers and consumers of the regulated materials also decreased their paperwork. They also were able to better match supply of materials with demand for them, since authorized organizations could retrieve information about the quantities present at each site.

The operations phase also included security monitoring. All participating organizations signed a MOU that included sharing of information pertaining to possible intrusions or security exploits. This close cooperation enabled one of the suppliers and a national laboratory to recognize a recurring attack pattern across facilities that might otherwise have been ignored. As a result, two members of an underground computer user group were arrested.

8.2.5 Phase 5: Disposition

As a new program, RTA has not actively confronted disposition issues. It plans to instruct participating organizations to retire their RFID systems as they would any other system holding data that RTA deems sensitive. In most cases this involves using disk wiping utilities to delete sensitive files. With regard to tag disposition, RTA's position is that organizations are free to recycle tags so long as they clear sensor and manifest data before affixing a tag to a new item.

8.2.6 Summary and Evaluation

The RTA RFID initiative allowed the agency to exercise more effective oversight of the transportation of radionuclide material while also reducing the regulatory compliance cost of impacted organizations. Some important security concerns had been raised, particularly with regards to the possibility that an adversary might use the RFID tags as targeting devices. Early identification of these risks allowed them to be managed during the each stage of the systems lifecycle. A listing of the main risks and the corresponding mitigation approach is presented in Table 8-2.

Table 8-2. RTA Risk Management Strategy

Risk	Mitigation Approach
Targeting of transport vehicles	• Shielding of vehicles and containers to prevent electromagnetic emissions
Eavesdropping to gather intelligence	• Physical facility perimeter at least 100 meters from storage locations
Disabling tags to allow material movement to go undetected	• Shielding during transport • Physical access controls
Altering sensor or manifest data stored on the tag to undermine mission	• Shielding during transport • Physical access controls • Password-based authentication for write transactions
Corruption of tag naming service	• Limit access to naming service to private network hosts

Risk	Mitigation Approach
Combustion of collocated volatile materials	• Use of less risk-prone radio frequency (i.e., HF) • Five meter separation between tags and volatile materials

Appendix A—RFID Standards and Frequency Regulations

RFID interrogators and tags must conform to the same standards and designs to be interoperable. These standards and designs also can be used to coordinate the use of certain tags across multiple enterprises and in the supply chain. Common standards and designs may facilitate training, future equipment procurement, and equipment upgrades. Some interrogators and some tags can operate using multiple standards. This appendix describes national and international standards, industrial standards, and proprietary designs for RFID systems. It also discusses regulations for frequencies used by various RFID standards and non-standard implementations.

A.1 International Standards

RFID standards have been developed by national and international standards groups such as the ISO. There are separate standards for contactless smart cards and for item management.

ISO 14443 and ISO 15693 are the most popular smart card standards.

- ISO 14443 describes proximity smart cards which have an intermediate range up to 10 cm and operate at 13.56 MHz. The standard contains four parts: (1) physical characteristics, (2) radio frequency power and signaling, (3) initialization and anti-collision, and (4) transmission protocols. ISO 14443 has two variants known as ISO 14443A and ISO 14443B which have different communications interfaces. Interrogators that are ISO 14443 compliant must be able to communicate using ISO 14443A and ISO 14443B. ISO 14443A parts 1 through 4 are used in the Department of Defense Common Access Card (CAC) which serves as an identification card. The CAC has a FIPS-approved algorithm.

- ISO 15693 operates at 13.56 MHz and describes vicinity smart cards which can be read from a farther distance than close coupled or proximity cards. Such cards have a range of up to approximately 1 m.

ISO 18000 is an RFID standard for item management and describes the air interface for various frequencies. Each standard within the ISO 18000 family defines communications parameters and applies to a specific electromagnetic frequency. ISO 18000-1 covers general parameters, and ISO 18000-2 through 18000-7 cover specifics for particular frequency ranges.

- ISO 18000-2 covers frequencies below 135 kHz. It has two types, A (Full Duplex) and B (Half Duplex). These types are different on the physical layer. Full duplex tags are always powered by the interrogator. Half duplex tags are powered by the interrogator except when the tags communicate to the interrogator.

- ISO 18000-3 covers frequencies operating at 13.56 MHz and describes two non-interfering and not interoperable modes of operation. Users are recommended to use just one mode for any single application. Both modes use a 64-bit identifier.

  - Mode 1 has a locking feature that is not protected by password. If the tag receives the *lock* command, it locks the corresponding area of memory permanently. *Lock* can be applied selectively to different areas of memory.

  - Mode 2 has a 48-bit password used to protect memory access. The tag can be configured to require or not require this password. If required, then *read* and *write* commands will require the interrogator to issue the correct 48-bit password. Mode 2 has a 16-bit lock pointer which is located in unaddressable memory. The lock points to a word in memory. All complete

blocks of memory at addresses less than the number stored in the lock pointer cannot be overwritten.

- ISO 18000-4 covers systems operating at 2.45 GHz. This standard has two modes: a passive tag interrogator-talks-first mode, and a battery assisted tags-talks-first mode.
- ISO 18000-5 was developed for 5.8 GHz operation but this standard was withdrawn.
- ISO 18000-6 has Types A and B. Both Type A and B operate at 860 to 930 MHz, but they use different encoding and anti-collision methods in the forward link. ISO has ratified the EPCglobal Class-1 Generation-2 standard as ISO 18000-6 Type C.
- ISO 18000-7 is an ITF protocol for an RFID system that operates at 433 MHz. Tags have a 32-bit tag ID and a 16-bit manufacturer ID. Interrogators are given a 16-bit identifier as well. A 32-bit password can be set on the tags. A secure byte is set to determine if the tag is password protected or not. If protected, read/write of the User ID, User ID Length, Routing Code, and memory is password protected. ISO 18000-7 supports optional command database query commands that are transmitted to all tags. The queries are sent in multiple steps and can use logical operators such as clear, and, and or, and relational operators such as equal, less than, greater than, and not. Tags that receive all steps of the query will do an internal database search and interrogators can retrieve the results of these queries.

There are also a number of item management-related standards for the application of livestock tracking.[76]

A.2 Industry Standards

The most prominent industry standards for RFID are the EPCglobal[77] specifications and standards for supply chain applications. These specifications use an identifier intended for the global supply chain known as the EPC. All EPC specifications developed to date are for passive, interrogator-talks-first RFID systems. Four specifications have been developed by EPCglobal: Class-0 UHF, the Class-1 Generation-1 HF, the Class-1 Generation-1 UHF, and the Class-1 Generation-2 UHF specifications. Of these specifications, the Class-1 Generation-2 specification has been approved by EPCglobal as a standard.

The first specification developed by EPCglobal was the EPC Class-0 specification for 900 MHz UHF operation. The intent of this specification was to establish a low cost identification tag. The Class-0 specification provides three main features: an EPC, a 16-bit cyclic redundancy check (CRC),[78] and a self-destruct feature. The self-destruct feature is also known as the kill feature. When an interrogator issues the *kill* command and the appropriate 24-bit password, the tag no longer responds to any commands. [79] The Four EPC identifiers presented in the standard are shown in Table A-1.

[76] Livestock tracking standards include ISO 11784, ISO 11785, and ISO 14223. ISO 11784 covers the data format for such tags. ISO 11785 designs the technical details of such a tag, and ISO 14223 is an updated standard for livestock tracking tags.

[77] EPCglobal is a joint venture between Global Standards One (GS1), which was formerly known as European Article Numbering (EAN) International, and GS1 US, which was formerly known as the Uniform Code Council (UCC), Inc.).

[78] A cyclic redundancy check is used to detect errors such as those introduced by noise in a communication channel.

[79] Auto-ID Center. Draft proposal specification for a 900 MHz Class 0 Radio Frequency Identification Tag. Feb 23, 2003. http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

Table A-1. EPC Identifier Formats

EPC Type	Header Size	First Bits	Domain Manager	Object Class	Serial Number	Total
64 bit Type I	2	01	21	17	24	64
64 bit Type II	2	10	15	13	34	64
64 bit Type III	2	11	26	13	23	64
96 bit and more	8	00	28	24	36	96

Next, two EPCglobal Class-1 Generation-1 specifications were developed: one for HF operation and one for UHF operation. The HF specification defines a tag that operates at 13.56 MHz and has three main features: an EPC, a 16-bit cyclic redundancy check, and a self-destruct feature. Its *kill* code is 24 bits.[80] There currently are no commercial products based on the EPCglobal Class-1 Generation-1 specification for 13.56 MHz and nearly all references to EPC Class-1 Generation-1 tags refer to the UHF specification. This is because 13.56 MHz offers operating ranges of up to one meter, which is not as useful in item management as UHF, which can offer operating ranges of several meters. The UHF specification defines a tag that operates at 860 MHz – 960 MHz and has an EPC identifier, an error detection code, and a *kill* command. The EPC shall be a valid EPC that contains four subfields: a Header/Version, a Domain Manager, an Object Class, and a Serial number. The error detection is performed using a 16-bit CRC. The *kill* password is 8 bits.[81]

The EPCglobal Class-1 Generation-2 standard is the only specification that became a standard ratified by EPCglobal.[82] The previous Class-0 and Class-1 Generation-1 tags are expected to be phased out and replaced by Class-1 Generation-2 tags. It describes tags with five major features: an EPC, a tag identifier (TID), a *kill* command, an optional password-protected access control, and an optional user memory. The tag identifier is used to identify the design and features of the individual tag. This is necessary since tags may have optional or custom commands and features. Cyclic redundancy checks are used in some communications and for the EPC. There is a 32-bit *kill* password and a 32-bit access password. The standard also implements a *lock* command which can temporarily or permanently make an area of memory write protected or read and write protected.[83]

EPCglobal Class-1 Generation-2 tags also use a cover-coding method to obscure information that is sent from an interrogator to a tag. Cover-coding generates cipher text by performing a bit-wise XOR operation between 16 bits of plain text and 16 bits of a random number key. The plain text is recovered by performing another bit-wise XOR between the 16 bits of cipher text and the same 16 bit random number key. Three things are cover-coded when they are sent from the interrogator to the tag: data written using the *write* command, the access password, and the *kill* password.

To initiate cover-coding, the interrogator commands the tag to generate a 16 bit random number. The tag does this and backscatters the random number to the interrogator. The interrogator uses this random

---

80 Auto-ID Center. Technical Report: 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0. Feb. 1, 2003. http://www.epcglobalinc.org/standards_technology/Secure/v1.0/HF-Class1.pdf

81 Auto-ID Center. Technical Report: 860 MHz – 960 MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1. Nov 14, 2002. http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

82 This standard is expected to be adopted with minor changes as the ISO/International Electrotechnical Commission (IEC) 18000-6C.

83 EPCglobal. EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz. Version 1.0.9. Jan. 31, 2005. http://www.epcglobalinc.org/standards_technology/EPCglobalClass-1Generation-2UHFRFIDProtocolV109.pdf

number as a key and performs the first bit-wise XOR between 16 bits of plain text and the 16 bit random number key. This generates 16 bits of cipher text which is subsequently sent over the air to the tag. The tag can uncover the cipher text by performing another bit-wise XOR between the 16 bits of cipher text and the original 16 bit random number.

Figure A-1 illustrates the utility of this cover-coding. As shown in the figure below, in passive RFID systems interrogators have substantially longer transmission ranges than tags. Passive tags modulate and backscatter the interrogator's signal to communicate. Therefore, passive tag transmissions have only a fraction of the power of interrogator transmissions and have a more limited transmission range and are less susceptible to eavesdropping.

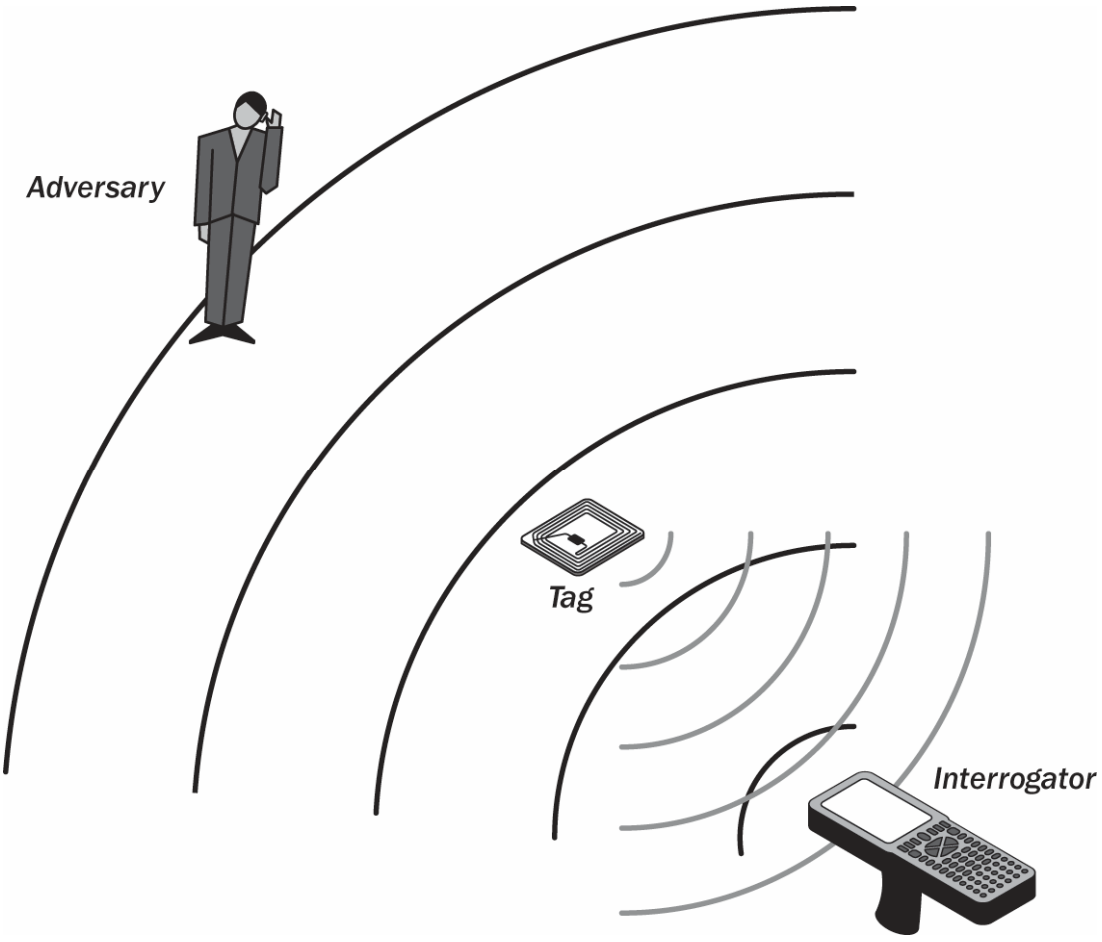

Figure A-1. Cover-Coding

As a result of these transmission ranges, the cover-coding technique is effective only when an adversary cannot intercept the tag's backscattered signals. In such a scenario, the adversary will be able to hear the interrogator ask the tag for a random number to use as a key in cover-coding,, but the adversary will not be able to hear the response – i.e., the random number that the tag transmits back to the interrogator. The interrogator will successfully receive the random number key from the tag. The interrogator will be able to create the cover-coded cipher text. Then when the interrogator transmits the cipher text, the tag will be able to uncover the cipher text using the random number. The adversary will not be able to uncover the cipher text because the adversary is too far from the tag to have heard the tag transmit the random number key.

A.3 Security Features in RFID Standards

Table A-2 provides an overview of the security features offered by several RFID standards.

Table A-2. Security Features in RFID Standards

RFID Standard (application)	Technical Features			Security Features		
	Band	Range (m)	Data	Confidentiality	Integrity	Availability
EPC Class-0/0+ (supply chain)	UHF	3	64 or 96-bit with read/write (R/W) block	None in standard	Parity bit CRC error detection	Identification rate > 1000 tags/sec
EPC Class-1 Generation-1 (supply chain)	UHF	3	64 or 96-bit with R/W block	None in standard	Commands have 5 parity bits CRC error detection	*Lock* command permanent and not protected
EPC Class-1 Generation-2 (supply chain)	UHF	3	R/W block	Masked reader-to-tag communications using the one-time pad stream cipher Tags addressed by 16-bit random numbers	CRC error detection	Numerous readers can operate in dense configurations
ISO/IEC 18000-2 (item management)	LF	< 0.010	Up to 1 Kbyte R/W	No protection on the *read* command "Reader talks first" protocol No encryption or authentication	CRC error detection Permanent, factory set 64-bit ID Optional, lockable identifier code	None in standard
ISO/IEC 18000-3 (item management)	HF	< 2	R/W	"Reader talks first" protocol 48-bit password protection on *read* commands "Quiet mode" in which tags will not respond to readers	CRC error detection No write protection in Mode 1 Mode 2 has 48-bit password on *write* commands	Multiple tag modes are non-interfering
ISO/IEC 11784-11785 (animal tracking)	LF	< 0.010	64-bit identifier	"Reader talks first" protocol Tags addressed by 16-bit random numbers Quiet mode	Retagging counter CRC error detection	None in standard

RFID Standard (application)	Technical Features			Security Features		
	Band	Range (m)	Data	Confidentiality	Integrity	Availability
ISO/IEC 10536 (contactless smart cards)	HF	< 2	R/W	"Reader talks first" protocol Masked reader-to-tag communications Tags addressed by random number Quiet mode	CRC error detection	Probabilistic/slotted random anti-collision algorithm Multiple tag modes are non-interfering
ISO/IEC 14443 (contactless smart cards)	HF	≈ 0.07 to 0.15	Type A: 32, 56, or 80 bit identifier Type B: 32 bit identifier	N/A[84]	CRC error detection	Type A: binary search tree anti-collision Type B: slotted Aloha anti-collision protocol
ISO/IEC 15693 (vicinity smart cards)	HF	1.5	Up to 1 Kbyte R/W	No protection on the *read* command No onboard encryption or authentication	Optional protections on *write* command Error checking on air interface	Optional password protection on the *lock* command

A.4 Proprietary Designs

Numerous companies have created their own proprietary RFID tag designs, many of which are based on open standards. In the case of proprietary designs, readers of this document are encouraged to seek information from the vendors about these products.

Two prominent examples of proprietary tags that are, in effect, proprietary extensions of open standards, but offer extended features are item management tags and contactless smart cards. Item management tags that are based on the air interface defined by ISO 18000-7 are widely used to monitor shipments of cargo containers. These tags have found widespread use by the U.S. Department of Defense to track military cargo. Proprietary tags based on ISO 18000-7 operate at 433 MHz, can have a range of 300 feet, and can have user memories up to 128 Kbytes. Contactless smart cards are often based on ISO 14443; such tags are widely used in public transportation and can also be used in access control, financial payment, gaming, loyalty card programs, and toll road payment. Many contactless smart cards are enhanced with proprietary extensions and security features.

[84] While the ISO 14443 itself does not provide confidentiality services, these services are available in many applications that use ISO 14443 for wireless communications.

Appendix B—Glossary

Selected terms used in *Guidance for Securing Radio Frequency Identification (RFID) Systems* are defined below.

Active Tag: A tag that relies on an internal battery for power.

Analytic Software: Software that is used to interpret and process data collected by an RFID system.

Blocker Tag: A special tag that prevents unauthorized interrogators from communicating with tags within range. Blocker tags confuse interrogators during singulation so that they cannot identify individual tags.

Cloned Tag: A tag that is made to be a duplicate of a legitimate tag. A cloned tag can be created by reading data such as an identifier from a legitimate tag and writing it to a different tag.

Eavesdropper: A party that secretly receives communications intended for others.

Electronic Product Code Identifier: One of the available formats for encoding identifiers on tags. EPC identifiers describe the class of object, the serial number, and the organization responsible for assigning the class and serial number.

Electronic Product Code Information Services: An inter-enterprise subsystem that facilitates information sharing using the EPCglobal network. EPCISs can query one another for information about products with EPC identifiers.

Enterprise Subsystem: Processes information collected by the RF subsystem's interrogators. The enterprise subsystem relies on middleware and analytic software to process and interpret the information. Enterprise subsystems are used to store large amounts of information about individual assets or people.

Inter-Enterprise Subsystem: Enables sharing of information across organizations through a networking implementation between the organizations' enterprise subsystems. It can include a discovery service to facilitate looking up information on specific identifiers.

Interrogator: A device that can wirelessly communicate with tags. Interrogators can detect the presence of tags as well as send and receive data and commands from the tags.

Interrogator Jamming: A deliberate communications disruption meant to degrade the operational performance of an interrogator. Jamming is achieved by interjecting electromagnetic waves on the same frequency that the interrogator uses for communication.

Interrogator Spoofing: The act of impersonating a legitimate interrogator of an RFID system to read tags.

Interrogator Talks First: An RF transaction in which the interrogator transmits a signal that is received by tags in its vicinity. The tags may be commanded to respond to the interrogator and continue with further transactions.

***Kill* Command:** A command that interrogators can send to tags that uses electronic disabling mechanisms to prevent tags from responding to any additional commands.

***Lock* Command:** A command that interrogators can send to a tag to block access to certain information on the tag.

Middleware: Software that can be used to aggregate and filter the large amounts of data collected by RFID interrogators and then pass the information to a database of the enterprise subsystem. Middleware is also responsible for monitoring and managing interrogators and printers.

Network Services: Provide communication channels between the RF and enterprise subsystems as well as between the components of the enterprise subsystem.

Object Naming Service: A proposed inter-enterprise subsystem that will act as a global network to store a look up table of RFID identifiers and corresponding network addresses where more information about that identifier can be obtained.

Passive Tag: A tag that does not have its own power supply. Instead, it uses RF energy from the interrogator for power. Due to the lower power, passive tags have shorter ranges than other tags, but are generally smaller, lighter, and cheaper than other tags.

Radio Frequency Identification: A technology used for wireless identification of assets or people. It is similar to the use of UPC bar codes on retail merchandise, but it is used to provide more in-depth information and has a longer range. Tags are associated with individual assets or people so that interrogators can then wirelessly identify them.

Radio Frequency Subsystem: Composed of tags and interrogators and operates at the edge of the enterprise subsystem's network. RFID subsystems wirelessly identify assets and people using tags.

Semi-Active Tag: A tag that uses a battery to communicate but remains dormant until an interrogator sends an energizing signal. Semi-active tags have a longer range than passive tags and a longer battery life than active tags.

Semi-Passive Tag: A tag that communicates the same way as passive tags without consuming battery power. Semi-passive tags also contain batteries to support sensors or cryptographic modules.

Skimming: The unauthorized use of an interrogator to read tags without the authorization or knowledge of tag's owner or the individual in possession of the tag.

Shrinkage: Declining revenue due to loss or theft of products.

Singulation: A function performed by an interrogator to individually identify any tags in the interrogator's operating range.

Smart Card: A pocket-sized card that contains integrated circuits. Such cards may be capable of functioning as RFID tags.

Tag: An electronic device that can communicate with RFID interrogators. A tag can function as a beacon or it can be used to convey information such as an identifier.

Tag Talks First: An RF transaction in which the tag communicates its presence to an interrogator. The interrogator may then send commands to the tag.

Appendix C—Acronyms and Abbreviations

Selected acronyms and abbreviations used in *Guidance for Securing Radio Frequency Identification (RFID) Systems* are defined below.

ACL	Access Control List
AIDC	Automatic Identification and Data Capture
AIT	Automatic Identification Technology
BLPR	Baseline Privacy Requirements
CAC	Common Access Card
CD-ROM	Compact Disc Read Only Memory
cm	Centimeters
CIO	Chief Information Officer
CRC	(fictional) Contagion Research Center
CRC	Cyclic Redundancy Check
CSO	Chief Security Officer
CSRC	Computer Security Resource Center
DNS	Domain Name System
DoD	Department of Defense
E3	Electromagnetic Environmental Effects
EAN	European Article Number
EAS	Electronic Article Surveillance
EIRP	Effective Isotropic Radiated Power
EPC	Electronic Product Code
EPCIS	Electronic Product Code Information Services
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FOIA	Freedom of Information Act
FY	Fiscal Year
GHz	Gigahertz
GRS	General Records Schedule
GS1	Global Standards One
GSA	General Services Administration
HERF	Hazards of Electromagnetic Radiation to Fuel
HERO	Hazards of Electromagnetic Radiation to Ordnance
HERP	Hazards of Electromagnetic Radiation to People
HF	High Frequency
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
Hz	Hertz
ID	Identifier
IEC	International Electrotechnical Commission

IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPsec	Internet Protocol Security
ISM	Industrial, Scientific, and Medical
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
ITF	Interrogator Talks First
kHz	Kilohertz
LAN	Local Area Network
LF	Low Frequency
m	Meter
MHz	Megahertz
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MRI	Magnetic Resonance Imaging
MX	Mail Exchanger
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCIO	Office of the Chief Information Officer
OECD	Organization for Economic Cooperation and Development
OMB	Office of Management and Budget
ONS	Object Naming Service
OSHA	Occupation Safety and Health Administration
PUB	Publication
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
RF	Radio Frequency
RFID	Radio Frequency Identification
RTA	(fictional) Radionuclide Transportation Agency
RTLS	Real-Time Location System
R/W	Read/Write
SDLC	System Development Lifecycle
SNMP	Simple Network Management Protocol
SP	Special Publication
SSL	Secure Sockets Layer
SSN	Social Security Number
TCP	Transmission Control Protocol
TID	Tag Identifier
TLS	Transport Layer Security
TTF	Tag Talks First

UCC	Uniform Code Council
UHF	Ultra High Frequency
UPC	Universal Product Code
URI	Uniform Resource Identifier
URL	Universal Resource Locator
VHF	Very High Frequency
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WORM	Write once, read many
WPA	Wi-Fi Protected Access
WSDL	Web Services Description Language
XOR	Exclusive-or

This page has been left blank intentionally.

Appendix D— Information Resources

The lists below contain information resources that may be helpful for organizations planning or operating RFID systems.

Print Publications and Books

American National Standard. *IDE standard for safety levels with respect to human exposure to radio frequency electromagnetic fields*, 3 kHz to 300 GHz, IEEE C95.1 – 1991, April 1992.

Finkenzeller, Klaus, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards and Identification*, John Wiley & Sons, 2003.

Garfinkel, Simson and Rosenberg, Beth, *RFID Applications, Security, and Privacy*, Addison-Wesley Professional, 2005.

Glover, Bill and Bhatt, Hiimanshu, *RFID Essentials*, O'Reilly, 2006.

Lahiri, Sandip, *RFID Sourcebook*, IBM Press, 2005.

Articles and Other Published Materials

29 CFR 1910.97.
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9745

Auto-ID Center, "Draft proposal specification for a 900 MHz Class 0 Radio Frequency Identification Tag", Feb 23, 2003.
http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class0.pdf

Auto-ID Center, "Technical Report: 13.56 MHz ISM Band Class 1 Radio Frequency Identification Tag Interface Specification: Candidate Recommendation, Version 1.0.0", Feb. 1, 2003. http://www.epcglobalinc.org/standards_technology/Secure/v1.0/HF-Class1.pdf

Auto-ID Center, "Technical Report: 860 MHz – 960 MHz Class I Radio Frequency Identification Tag Radio Frequency & Logical Communication Interface Specification Candidate Recommendation, Version 1.0.1", Nov 14, 2002.
http://www.epcglobalinc.org/standards_technology/Secure/v1.0/UHF-class1.pdf

"The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy" in V. Atluri, ed. 8th ACM Conference on Computer and Communications Security, ACM Press, 2003, pp. 103-111.

Brower, Katherine and Henderson, William, "In Your Pocket: Using Smart Cards for Seamless Travel", Permanent Citizens Advisory Committee to the MTA, October 2004.

DoD Directive 3222.3, "DoD Electromagnetic Environmental Effects (E3) Program," September 8, 2004.

EPCglobal, "EPC Radio-Frequency Identity Protocols Class-1 Generation-2 UHF RFID Protocol for Communications at 860 MHz – 960 MHz, Version 1.0.9", Jan. 31, 2005.

http://www.epcglobalinc.org/standards_technology/EPCglobalClass-1Generation-2UHFRFIDProtocolV109.pdf

EPCglobal, "Guidelines on EPC for Consumer Products". http://www.epcglobalinc.org/public/ppsc_guide/. Accessed on August 22, 2006.

Federal Communications Commission Office of Engineering and Technology, "OET Bulletin 56, Fourth Edition", August 1999, pp. 6-7, p. 26.

Federal Communications Commission Part 15 Section 247.

"FIFA boots chip ball from 2006 soccer World Cup", December 6, 2006, http://www.infoworld.com/article/05/12/06/HNfifaboots_1.html.

Garfinkel, Simson, "Adopting Fair Information Practices to Low Cost RFID Systems", paper presented at Privacy in Ubicomp 2002 workshop, Gotenborg, Sweden, September 29th, 2002. http://www.simson.net/clips/academic/2002.Ubicomp_RFID.pdf. Accessed August 22, 2006.

Juels, A, "RFID Security and Privacy: A Research Survey," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, February 2006, pp. 381-394.

Kirschenbaum, Ilan and Wool, Avishai, "How to Build a Low-Cost, Extended-Range RFID Skimmer", February 2, 2006, http://eprint.iacr.org/2006/054.pdf.

Navy AIT Program Office, Naval Supply Systems Command, "Navy Automatic Identification Technology (AIT) Program Office Value Chain Demonstration Phase 1", January 27, 2006.

"Position Statement on the Use of RFID on Consumer Products". http://www.privacyrights.org/ar/RFIDposition.htm. Accessed August 22, 2006.

Roberti, Mark, "FDA Tests RFID's Effect on Insulin", RFID Journal, Oct. 31, 2005. http://www.rfidjournal.com/article/articleprint/1961/-1/1/

Shamir, A., "Power Analysis of RFID Tags," presented at RSA Conference 2006, San Jose, CA, 2006. http://www.wisdom.weizmann.ac.il/~yossio/rfid/

Sullivan, Laurie, "IBM Shares Lessons Learned From Wal-Mart RFID Deployment", InformationWeek, Oct 15, 2004.

Tanenbaum, Andrew S., "Is Your Cat Infected with a Computer Virus?", Vrije Universiteit Amsterdam, Computer Systems Group, March 15, 2006.

Texas Instruments, "Automotive Immobilizer Anti-Theft System Experience Rapid Growth in 1999", June 1, 1999. http://www.ti.com/tiris/docs/news/news_releases/90s/rel06-01-99.shtml

Wynne, Michael, "Radio Frequency Identification (RFID) Policy", Jul 30, 2004. http://www.acq.osd.mil/log/rfid/Policy/RFID%20Policy%2007-30-2004.pdf

Internet Resources

Organization	URL
Auto-ID Labs	http://www.autoidlabs.org/
Automatic Identification Technology Office	http://www.dodait.com/
EPCglobal	http://www.epcglobalinc.org/
FCC OET Bulletins #56 and #65	http://www.fcc.gov/oet/info/documents/bulletins/
GSA Smart Card Web Site	http://www.smart.gov/
International Organization for Standardization	http://www.iso.org/
NIST Computer Security Guidance Publications	http://csrc.nist.gov/publications/
RFID Journal	http://www.rfidjournal.com/

General NIST Security Resources

Document	URL
FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*	http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
SP 800-12, *An Introduction to Computer Security: The NIST Handbook*	http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf
SP 800-14, *Generally Accepted Principles and Practices for Securing Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
SP 800-30, *Risk Management Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf
SP 800-31, *Intrusion Detection Systems*	http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf
SP 800-34, *Contingency Planning Guide for Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf
SP 800-35, *Guide to Information Technology Security Services*	http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf
SP 800-40v2, *Creating a Patch and Vulnerability Management Program*	http://csrc.nist.gov/publications/nistpubs/800-40-Ver2/SP800-40v2.pdf
SP 800-41, *Guide to Firewall Selection and Policy Recommendations*	http://csrc.nist.gov/publications/nistpubs/800-41/sp800-41.pdf
SP 800-44, *Guidelines on Securing Public Web Servers*	http://csrc.nist.gov/publications/nistpubs/800-44/sp800-44.pdf
SP 800-47, *Security Guide for Interconnecting Information Technology Systems*	http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf
SP 800-48, *Wireless Network Security: 802.11, Bluetooth, and Handheld Devices*	http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
SP 800-50, *Building an Information Technology Security Awareness and Training Program*	http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf
SP 800-53, *Recommended Security Controls for Federal Information Systems*	http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf
SP 800-64, *Security Considerations in the Information System Development Life Cycle*	http://csrc.nist.gov/publications/nistpubs/800-64/NIST-SP800-64.pdf

Document	URL
SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*	http://csrc.nist.gov/publications/nistpubs/800-65/SP-800-65-Final.pdf
SP 800-68, *Guidance for Securing Microsoft Windows XP Systems for IT Professionals*	http://csrc.nist.gov/itsec/download_WinXP.html
SP 800-70, *The NIST Security Configuration Checklists Program*	http://csrc.nist.gov/checklists/download_sp800-70.html
SP 800-77, *Guide to IPsec VPNs*	http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf
SP 800-97, *Guide to IEEE 802.11i: Robust Security Networks (DRAFT)*	http://csrc.nist.gov/publications/drafts/Draft-SP800-97.pdf